日　本　国　特　許　庁
JAPAN PATENT OFFICE

別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office

出願年月日
Date of Application: ２００２年　７月２３日

出願番号
Application Number: 特願２００２－２１３７０１

[ST.10/C]: [ＪＰ２００２－２１３７０１]

出願人
Applicant(s): ソニー株式会社

２００３年　６月　２日

特許庁長官
Commissioner,
Japan Patent Office 太田信一郎

出証番号　出証特２００３－３０４２４５９

【書類名】　特許願

【整理番号】　0290549406

【提出日】　平成14年 7月23日

【あて先】　特許庁長官殿

【国際特許分類】　H04L　9/00

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　栗屋　志伸

【発明者】

【住所又は居所】　東京都品川区北品川６丁目７番３５号　ソニー株式会社内

【氏名】　北谷　義道

【特許出願人】

【識別番号】　000002185

【氏名又は名称】　ソニー株式会社

【代理人】

【識別番号】　100093241

【弁理士】

【氏名又は名称】　宮田　正昭

【電話番号】　03-5541-7577

【選任した代理人】

【識別番号】　100101801

【弁理士】

【氏名又は名称】　山田　英治

【電話番号】　03-5541-7577

【選任した代理人】

【識別番号】　100086531

【弁理士】

【氏名又は名称】　澤田　俊夫

【電話番号】　03-5541-7577

【手数料の表示】

【予納台帳番号】　048747

【納付金額】　21,000円

【提出物件の目録】

【物件名】　明細書　1

【物件名】　図面　1

【物件名】　要約書　1

【包括委任状番号】　9904833

【プルーフの要否】　要

【書類名】　明細書

【発明の名称】　情報処理装置、および情報処理方法、並びにコンピュータ・プログラム

【特許請求の範囲】

【請求項１】

暗号化コンテンツの復号および再生処理を実行するクライアントとしての情報処理装置であり、

ライセンス情報としてのコンテンツ利用権情報に従ったコンテンツ利用処理を実行する制御手段を有し、

前記制御手段は、

購入済みのコンテンツまたは取得済みのライセンス情報についての再取得処理の実行に際し、再取得処理に適用するリストア処理要求ファイルとして、有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つデータファイルを生成し、生成したリストア処理要求ファイルをクライアント識別データとして適用することにより、前記購入済みのコンテンツまたは取得済みのライセンス情報の再取得を実行する構成を有することを特徴とする情報処理装置。

【請求項２】

前記制御部の生成するリーフＩＤに対する検証データは、リーフＩＤを入力データとして、秘密鍵によって生成したハッシュ値であり、前記秘密鍵は、コンテンツまたはライセンス情報の再取得要求の検証先において共有する秘密鍵であることを特徴とする請求項１に記載の情報処理装置。

【請求項３】

前記制御部の生成するリーフＩＤに対する検証データは、リーフＩＤを入力データとして、秘密鍵によって生成したＭＡＣ値であり、前記秘密鍵は、コンテンツまたはライセンス情報の再取得要求の検証先において共有する秘密鍵であることを特徴とする請求項１に記載の情報処理装置。

【請求項４】

前記制御手段は、

有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つ前記リストア処理要求ファイルを再取得要求の検証先に対してアップロードする処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項５】

前記ライセンス情報は、ライセンスサーバから提供されるサービスデータを含み、

前記制御部は、

前記サービスデータに格納されたデバイスノードキー（ＤＮＫ）を含む有効化キーブロック（ＥＫＢ）の処理を実行して、暗号化コンテンツの復号処理に適用するコンテンツキーＫｃを取得する処理を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項６】

前記ライセンス情報は、ライセンスサーバから提供されるコンテンツ利用権情報であり、

前記制御部は、

前記利用権情報に格納されたコンテンツ識別子（ＣＩＤ）と再生対象コンテンツのコンテンツ識別子（ＣＩＤ）との一致を条件としてコンテンツ再生を実行する構成であることを特徴とする請求項１に記載の情報処理装置。

【請求項７】

コンテンツ再生を実行するクライアントからのコンテンツまたはライセンス情報についての再取得処理要求の受信に基づいて、再取得許可情報を出力する管理システムとしての情報処理装置であり、

有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つリストア処理要求ファイルをクライアントから受信し、受信したリストア処理要求ファイル内の検証データに基づく検証処理に基づくリストア処理要求の正当性確認を条件として再取得許可情報を出力する構成を有することを特徴とする情報処理装置。

【請求項８】

前記検証データは、リーフＩＤを入力データとして秘密鍵によって生成したハッシュ値であり、前記検証処理は、管理システムとしての情報処理装置の保有する秘密鍵を適用して生成したハッシュ値と、受信したリストア処理要求ファイル内の検証データとしてのハッシュ値との比較処理として行なう構成であることを特徴とする請求項７に記載の情報処理装置。

【請求項９】

前記検証データは、リーフＩＤを入力データとして秘密鍵によって生成したＭＡＣ値であり、前記検証処理は、管理システムとしての情報処理装置の保有する秘密鍵を適用して生成したＭＡＣ値と、受信したリストア処理要求ファイル内の検証データとしてのＭＡＣ値との比較処理として行なう構成であることを特徴とする請求項７に記載の情報処理装置。

【請求項１０】

暗号化コンテンツの復号および再生処理を実行するクライアントとしての情報処理装置における情報処理方法であり、

有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つリストア処理要求ファイルを生成するファイル生成ステップと、

前記リストア処理要求ファイルをクライアント識別データとして適用して購入済みのコンテンツまたは取得済みのライセンス情報の再取得処理を実行する情報再取得ステップと、

を有することを特徴とする情報処理方法。

【請求項１１】

前記ファイル生成ステップは、

リーフＩＤを入力として、コンテンツまたはライセンス情報の再取得要求の検証先において共有する秘密鍵を適用してハッシュ値を生成し、該ハッシュ値を検証データとする検証データ生成ステップを含むことを特徴とする請求項１０に記載の情報処理方法。

【請求項１２】

前記ファイル生成ステップは、

リーフＩＤを入力として、コンテンツまたはライセンス情報の再取得要求の検証先において共有する秘密鍵を適用してＭＡＣ値を生成し、該ＭＡＣ値を検証データとする検証データ生成ステップを含むことを特徴とする請求項１０に記載の情報処理方法。

【請求項１３】

前記情報処理方法は、さらに、

有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つ前記リストア処理要求ファイルを再取得要求の検証先に対してアップロードする処理を実行するステップを含むことを特徴とする請求項１０に記載の情報処理方法。

【請求項１４】

コンテンツ再生を実行するクライアントからのコンテンツまたはライセンス情報についての再取得処理要求の受信に基づいて、再取得許可情報を出力する管理システムとしての情報処理装置における情報処理方法であり、

有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つリストア処理要求ファイルをクライアントから受信するファイル受信ステップと、

受信したリストア処理要求ファイル内の検証データに基づく検証処理に基づくリストア処理要求の正当性確認実行する正当性確認処理ステップと、

前記正当性確認を条件として再取得許可情報を出力するステップと、

を有することを特徴とする情報処理方法。

【請求項１５】

前記検証データは、リーフＩＤを入力データとして秘密鍵によって生成したハッシュ値であり、前記正当性確認処理ステップは、

管理システムとしての情報処理装置の保有する秘密鍵を適用して生成したハッシュ値と、受信したリストア処理要求ファイル内の検証データとしてのハッシュ値との比較処理として行なうステップであることを特徴とする請求項１４に記載の情報処理方法。

【請求項１６】

前記検証データは、リーフＩＤを入力データとして秘密鍵によって生成したＭＡＣ値であり、前記正当性確認処理ステップは、

管理システムとしての情報処理装置の保有する秘密鍵を適用して生成したＭＡＣ値と、受信したリストア処理要求ファイル内の検証データとしてのＭＡＣ値との比較処理として行なうステップであることを特徴とする請求項１４に記載の情報処理方法。

【請求項１７】

暗号化コンテンツの復号および再生処理を実行するクライアントとしての情報処理装置における情報処理実行プログラムを記述したコンピュータ・プログラムであって、

有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つリストア処理要求ファイルを生成するファイル生成ステップと、

前記リストア処理要求ファイルをクライアント識別データとして適用して購入済みのコンテンツまたは取得済みのライセンス情報の再取得処理を実行する情報再取得ステップと、

を有することを特徴とするコンピュータ・プログラム。

【請求項１８】

コンテンツ再生を実行するクライアントからのコンテンツまたはライセンス情報についての再取得処理要求の受信に基づいて、再取得許可情報を出力する管理システムとしての情報処理装置における情報処理実行プログラムを記述したコンピュータ・プログラムであって、

有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つリストア処理要求ファイルをクライアントから受信するファイル受信ステップと、

受信したリストア処理要求ファイル内の検証データに基づく検証処理に基づくリストア処理要求の正当性確認実行する正当性確認処理ステップと、

前記正当性確認を条件として再取得許可情報を出力するステップと、

を有することを特徴とするコンピュータ・プログラム。

【発明の詳細な説明】

【０００１】

【発明の属する技術分野】

本発明は、情報処理装置、および情報処理方法、並びにコンピュータ・プログラムに関する。特に、クライアントが取得したコンテンツのバックアップデータの確保、リストア処理をセキュアに正当なクライアントに対して実行することを可能とした情報処理装置、および情報処理方法、並びにコンピュータ・プログラムに関する。

【０００２】

【従来の技術】

昨今、音楽データ、ゲームプログラム、画像データ等、様々なソフトウエアデータ（以下、これらをコンテンツ（Content）と呼ぶ）の、インターネット等のネットワーク、あるいは、メモリカード、ＨＤ、ＤＶＤ、ＣＤ等の流通可能な記憶媒体を介した流通が盛んになっている。これらの流通コンテンツは、ユーザの所有するＰＣ（Personal Computer）、記録再生器、再生専用器、あるいはゲーム機器内の記憶手段、例えばＨＤ，フラッシュメモリを有するカード型記憶装置、ＣＤ、ＤＶＤ等に格納され、再生処理が実行される。

【０００３】

記録再生装置、ゲーム機器、ＰＣ等の情報機器には、コンテンツをネットワークから受信するためのインタフェース、あるいはメモリカード、ＨＤ、ＤＶＤ、ＣＤ等にアクセスするためのインタフェースを有し、コンテンツの再生に必要となる制御手段、プログラム、データのメモリ領域として使用されるＲＡＭ、ＲＯＭ等を有する。

【０００４】

音楽データ、画像データ、あるいはプログラム等の様々なコンテンツは、再生機器として利用される記録再生装置、ゲーム機器、ＰＣ等の情報機器本体からのユーザ指示、あるいは接続された入力手段を介したユーザの指示により、例えば内蔵、あるいは着脱自在の記憶媒体から呼び出され、情報機器本体、あるいは接続されたディスプレイ、スピーカ等を通じて再生される。

【０００５】

ゲームプログラム、音楽データ、画像データ等、多くのソフトウエア・コンテンツは、一般的にその作成者、販売者に頒布権等が保有されている。従って、これらのコンテンツの配布に際しては、一定の利用制限、すなわち、正規なユーザに対してのみ、ソフトウェアの使用を許諾し、許可のない複製等が行われないようにする、すなわちセキュリティを考慮した構成をとるのが一般的となっている。

【０００６】

また、コンテンツと、コンテンツを利用する利用権とを独立に管理し、ユーザに提供する構成が提案されている。この構成において、ユーザは、例えば暗号化されたコンテンツを取得し、さらに、利用権データを購入することにより、利用権データから取得可能な鍵データ等に基づいて、暗号化コンテンツの復号用の鍵（コンテンツ鍵）を取得して、コンテンツを利用する。

【０００７】

利用権データには、ユーザのコンテンツ利用許可態様の設定情報が格納され、その許可情報において許された範囲でのコンテンツの利用が可能となるといったシステムが提案されている。

【０００８】

【発明が解決しようとする課題】

このように、コンテンツとコンテンツ利用権とを独立に管理し、ユーザに提供するシステムにおいては、コンテンツの利用、例えば音楽データ、画像データの再生、または配信、あるいはダウンロード処理に際して、利用権データのチェックが実行される。

【０００９】

このようなコンテンツ提供システムにおいて、クライアント側のコンテンツ再生システムとしてのＰＣ、携帯端末等の各種の情報処理装置に不具合が発生し、例えばコンテンツ利用権のアクセスが不可能になってしまうと、取得したコンテンツの再生が不可能になる場合が発生し得る。このような場合、現行のシステムにおいては、クライアントは、再度コンテンツの購入処理を行ない、あらたにコ

ンテンツに対応する利用権を取得することが必要となる。

【００１０】

クライアントが購入するコンテンツの中には、一度の購入処理により、その後の永久的なコンテンツ再生、利用権を付与するコンテンツも存在する。このようなコンテンツを購入したクライアントに対して、クライアントの装置の不具合によりコンテンツの再生が不可能になった場合、再度コンテンツ購入を余儀なくされることは問題である。

【００１１】

本発明は、このような状況に鑑みてなされたものであり、クライアントがコンテンツの正規な購入処理を行なって、正規に取得したコンテンツについて、コンテンツ利用権の紛失、あるいはアクセス不可といった事態が発生した場合であっても、コンテンツの利用、再生を実行可能とするように、コンテンツまたはコンテンツ利用権情報についてのバックアップデータの作成処理、リストア処理をセキュアに実行可能とするものであり、一定の制限の下に、正規なコンテンツ購入者であることの確認を条件として、バックアップデータの作成、リストアを可能とした情報処理装置、および情報処理方法、並びにコンピュータ・プログラムを提供することを目的とするものである。

【００１２】

【課題を解決するための手段】

本発明の第１の側面は、

暗号化コンテンツの復号および再生処理を実行するクライアントとしての情報処理装置であり、

ライセンス情報としてのコンテンツ利用権情報に従ったコンテンツ利用処理を実行する制御手段を有し、

前記制御手段は、

購入済みのコンテンツまたは取得済みのライセンス情報についての再取得処理の実行に際し、再取得処理に適用するリストア処理要求ファイルとして、有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つデータファイルを生成し、

生成したリストア処理要求ファイルをクライアント識別データとして適用することにより、前記購入済みのコンテンツまたは取得済みのライセンス情報の再取得を実行する構成を有することを特徴とする情報処理装置にある。

【００１３】

さらに、本発明の情報処理装置の一実施態様において、前記制御部の生成するリーフＩＤに対する検証データは、リーフＩＤを入力データとして、秘密鍵によって生成したハッシュ値であり、前記秘密鍵は、コンテンツまたはライセンス情報の再取得要求の検証先において共有する秘密鍵であることを特徴とする。

【００１４】

さらに、本発明の情報処理装置の一実施態様において、前記制御部の生成するリーフＩＤに対する検証データは、リーフＩＤを入力データとして、秘密鍵によって生成したＭＡＣ値であり、前記秘密鍵は、コンテンツまたはライセンス情報の再取得要求の検証先において共有する秘密鍵であることを特徴とする。

【００１５】

さらに、本発明の情報処理装置の一実施態様において、前記制御手段は、有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つ前記リストア処理要求ファイルを再取得要求の検証先に対してアップロードする処理を実行する構成であることを特徴とする。

【００１６】

さらに、本発明の情報処理装置の一実施態様において、前記ライセンス情報は、ライセンスサーバから提供されるサービスデータを含み、前記制御部は、前記サービスデータに格納されたデバイスノードキー（ＤＮＫ）を含む有効化キーブロック（ＥＫＢ）の処理を実行して、暗号化コンテンツの復号処理に適用するコンテンツキーＫｃを取得する処理を実行する構成であることを特徴とする。

【００１７】

さらに、本発明の情報処理装置の一実施態様において、前記ライセンス情報は、ライセンスサーバから提供されるコンテンツ利用権情報であり、前記制御部は、前記利用権情報に格納されたコンテンツ識別子（ＣＩＤ）と再生対象コンテン

ツのコンテンツ識別子（ＣＩＤ）との一致を条件としてコンテンツ再生を実行する構成であることを特徴とする。

【００１８】

さらに、本発明の第２の側面は、

コンテンツ再生を実行するクライアントからのコンテンツまたはライセンス情報についての再取得処理要求の受信に基づいて、再取得許可情報を出力する管理システムとしての情報処理装置であり、

有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つリストア処理要求ファイルをクライアントから受信し、受信したリストア処理要求ファイル内の検証データに基づく検証処理に基づくリストア処理要求の正当性確認を条件として再取得許可情報を出力する構成を有することを特徴とする情報処理装置にある。

【００１９】

さらに、本発明の情報処理装置の一実施態様において、前記検証データは、リーフＩＤを入力データとして秘密鍵によって生成したハッシュ値であり、前記検証処理は、管理システムとしての情報処理装置の保有する秘密鍵を適用して生成したハッシュ値と、受信したリストア処理要求ファイル内の検証データとしてのハッシュ値との比較処理として行なう構成であることを特徴とする。

【００２０】

さらに、本発明の情報処理装置の一実施態様において、前記検証データは、リーフＩＤを入力データとして秘密鍵によって生成したＭＡＣ値であり、前記検証処理は、管理システムとしての情報処理装置の保有する秘密鍵を適用して生成したＭＡＣ値と、受信したリストア処理要求ファイル内の検証データとしてのＭＡＣ値との比較処理として行なう構成であることを特徴とする。

【００２１】

さらに、本発明の第３の側面は、

暗号化コンテンツの復号および再生処理を実行するクライアントとしての情報処理装置における情報処理方法であり、

有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子として

のリーフＩＤおよび、該リーフＩＤに対する検証データを持つリストア処理要求ファイルを生成するファイル生成ステップと、

前記リストア処理要求ファイルをクライアント識別データとして適用して購入済みのコンテンツまたは取得済みのライセンス情報の再取得処理を実行する情報再取得ステップと、

を有することを特徴とする情報処理方法にある。

【００２２】

さらに、本発明の情報処理方法の一実施態様において、前記ファイル生成ステップは、リーフＩＤを入力として、コンテンツまたはライセンス情報の再取得要求の検証先において共有する秘密鍵を適用してハッシュ値を生成し、該ハッシュ値を検証データとする検証データ生成ステップを含むことを特徴とする。

【００２３】

さらに、本発明の情報処理方法の一実施態様において、前記ファイル生成ステップは、リーフＩＤを入力として、コンテンツまたはライセンス情報の再取得要求の検証先において共有する秘密鍵を適用してＭＡＣ値を生成し、該ＭＡＣ値を検証データとする検証データ生成ステップを含むことを特徴とする。

【００２４】

さらに、本発明の情報処理方法の一実施態様において、前記情報処理方法は、さらに、有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つ前記リストア処理要求ファイルを再取得要求の検証先に対してアップロードする処理を実行するステップを含むことを特徴とする。

【００２５】

さらに、本発明の第４の側面は、

コンテンツ再生を実行するクライアントからのコンテンツまたはライセンス情報についての再取得処理要求の受信に基づいて、再取得許可情報を出力する管理システムとしての情報処理装置における情報処理方法であり、

有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つリストア処理要求

ファイルをクライアントから受信するファイル受信ステップと、

受信したリストア処理要求ファイル内の検証データに基づく検証処理に基づくリストア処理要求の正当性確認実行する正当性確認処理ステップと、

前記正当性確認を条件として再取得許可情報を出力するステップと、

を有することを特徴とする情報処理方法にある。

【００２６】

さらに、本発明の情報処理方法の一実施態様において、前記検証データは、リーフＩＤを入力データとして秘密鍵によって生成したハッシュ値であり、前記正当性確認処理ステップは、管理システムとしての情報処理装置の保有する秘密鍵を適用して生成したハッシュ値と、受信したリストア処理要求ファイル内の検証データとしてのハッシュ値との比較処理として行なうステップであることを特徴とする。

【００２７】

さらに、本発明の情報処理方法の一実施態様において、前記検証データは、リーフＩＤを入力データとして秘密鍵によって生成したＭＡＣ値であり、前記正当性確認処理ステップは、管理システムとしての情報処理装置の保有する秘密鍵を適用して生成したＭＡＣ値と、受信したリストア処理要求ファイル内の検証データとしてのＭＡＣ値との比較処理として行なうステップであることを特徴とする。

【００２８】

さらに、本発明の第５の側面は、

暗号化コンテンツの復号および再生処理を実行するクライアントとしての情報処理装置における情報処理実行プログラムを記述したコンピュータ・プログラムであって、

有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つリストア処理要求ファイルを生成するファイル生成ステップと、

前記リストア処理要求ファイルをクライアント識別データとして適用して購入済みのコンテンツまたは取得済みのライセンス情報の再取得処理を実行する情報

再取得ステップと、

を有することを特徴とするコンピュータ・プログラムにある。

【００２９】

さらに、本発明の第６の側面は、

コンテンツ再生を実行するクライアントからのコンテンツまたはライセンス情報についての再取得処理要求の受信に基づいて、再取得許可情報を出力する管理システムとしての情報処理装置における情報処理実行プログラムを記述したコンピュータ・プログラムであって、

有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つリストア処理要求ファイルをクライアントから受信するファイル受信ステップと、

受信したリストア処理要求ファイル内の検証データに基づく検証処理に基づくリストア処理要求の正当性確認実行する正当性確認処理ステップと、

前記正当性確認を条件として再取得許可情報を出力するステップと、

を有することを特徴とするコンピュータ・プログラムにある。

【００３０】

【作用】

本発明の構成によれば、クライアントは、購入済みのコンテンツまたはライセンス情報としてのサービスデータ、または利用権情報を、正規なコンテンツ購入クライアントであることの確認を条件として、再取得可能となり、購入済みあるいは取得済みのデータの読み出しが不可能となった場合においてもバックアップされたデータに基づいて、コンテンツを利用することが可能となる。

【００３１】

さらに、本発明の構成によれば、クライアントは、購入済みのコンテンツまたはライセンス情報としてのサービスデータ、または利用権情報の再取得処理に際し、リストア処理要求ファイルとして、有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つデータファイルを生成し、生成したリストア処理要求ファイルをクライアント識別データとして適用する構成としたので、正規なコンテンツ

購入クライアントであることの確認が確実に実行される。

【００３２】

なお、本発明のコンピュータ・プログラムは、例えば、様々なプログラム・コードを実行可能な汎用コンピュータ・システムに対して、コンピュータ可読な形式で提供する記憶媒体、通信媒体、例えば、ＣＤやＦＤ、ＭＯなどの記憶媒体、あるいは、ネットワークなどの通信媒体によって提供可能なコンピュータ・プログラムである。このようなプログラムをコンピュータ可読な形式で提供することにより、コンピュータ・システム上でプログラムに応じた処理が実現される。

【００３３】

本発明のさらに他の目的、特徴や利点は、後述する本発明の実施例や添付する図面に基づくより詳細な説明によって明らかになるであろう。なお、本明細書においてシステムとは、複数の装置の論理的集合構成であり、各構成の装置が同一筐体内にあるものには限らない。

【００３４】

【発明の実施の形態】

以下、本発明の構成について詳細に説明する。なお、説明は、以下に示す各項目に従って行なう。

１．コンテンツ提供システム概要

２．キー配信構成としてのツリー（木）構造について

３．ＥＫＢを使用したキーの配布

４．ＥＫＢのフォーマット

５．ツリーのカテゴリ分類

６．コンテンツ購入および試聴処理

７．バックアップ／リストア処理

８．リコメンドファイルによるコンテンツの二次配信

【００３５】

［１．コンテンツ提供システム概要］

図１は、本発明を適用したコンテンツ提供システムの概要を説明する図である。コンテンツの利用を行なうクライアント１０は、コンテンツを利用、すなわち

再生可能な機器としての情報処理装置である。例えばＰＣ、ＰＤＡ等、各種の情報処理装置が含まれる。クライアント１０は、ソフトウェアとしてブラウザ１１、クライアントアプリケーション１２を有し、ＣＰＵ等の制御手段によりブラウザ１１、クライアントアプリケーション１２他のプログラムが実行される。

【００３６】

クライアントアプリケーション１２は、クライアントにおけるコンテンツの購入および試聴処理、後段において説明するサービスデータ、コンテンツ利用権情報を含むライセンス情報の取得処理、コンテンツおよびライセンス情報のバックアップ／リストア処理、コンテンツ利用権の確認処理、コンテンツ再生管理処理、あるいは、二次配信用のコンテンツファイルとしてのリコメンドファイルの生成処理等を実行するアプリケーションであり、以下、詳細に説明する処理プログラムとして、クライアントの情報処理装置に格納される。なお、本明細書においては、「試聴」は、音声データの試聴のみならず、画像データの試写を包含する意味として用いる。

【００３７】

クライアント１０は、例えばインターネット等の通信網を介してショップサーバ２１、ライセンスサーバ２２、およびコンテンツサーバ２３と接続される。コンテンツサーバ２３は、クライアント１０に対してコンテンツを提供する。ライセンスサーバ２２は、クライアントが利用するコンテンツの利用権情報をクライアント１０に対して提供する。また、ショップサーバ２１は、クライアント１０がコンテンツを購入する際の窓口として機能し、購入または試聴可能コンテンツをブラウザを介して提示し、クライアントからの購入あるいは試聴の要求を受け付ける。また、必要に応じて購入コンテンツに関する課金処理を行なう。

【００３８】

さらに、ショップサーバ２１、およびライセンスサーバ２２には、管理システム３１が接続される。管理システム３１は、ショップサーバ２１が受け付けたクライアント１０からのコンテンツ要求に対する許可情報として機能するトランザクションＩＤ（ＴＩＤ）の発行処理、コンテンツダウンロード許可情報の発行処理を行なう。また、管理システム３１は、ライセンスサーバ２２に対して、コン

ンツの利用権情報としての利用権データＵｓａｇｅ　Ｒｉｇｈｔ）の発行許可を行なう。これらの処理の詳細は、後段で説明する。

【００３９】

なお、クライアント１０は、ライセンスサーバ２２からの利用権の取得、コンテンツサーバ２３からのコンテンツ取得を、クライアントアプリケーション１２の制御の下に実行し、ショップサーバ２１の提供する情報の閲覧および決済処理は、クライアントアプリケーション１２の制御の下にブラウザ１１を起動して実行する。

【００４０】

図１には、クライアントおよび各サーバを１つづつ示してあるが、これらは例えばインターネット等の通信網上に多数接続され、クライアントは、様々なショップサーバに接続し、各ショップサーバで提供するコンテンツを自由に選択し、選択したコンテンツを格納したコンテンツサーバからコンテンツを取得し、取得したコンテンツの利用権を発行するライセンスサーバを選択して、その選択されたライセンスサーバから利用権を取得する。

【００４１】

コンテンツは、暗号化コンテンツとしてコンテンツサーバ２３からクライアント１０に提供される。さらに、ライセンスサーバ２２からクライアント１０に対しては、コンテンツに対応するコンテンツ利用権情報が提供され、クライアント１０のクライアントアプリケーション１２が、利用権情報を検証し、利用権があると判定された場合に暗号化コンテンツを復号して利用する。

【００４２】

クライアント１０は、コンテンツ利用権に基づくコンテンツ利用を可能とするための鍵情報として、有効化キーブロック（ＥＫＢ：Enabling Key Block）、デバイス・ノード・キー（ＤＮＫ：Device Node Key）等の鍵データを保持する。有効化キーブロック（ＥＫＢ：Enabling Key Block）、デバイス・ノード・キー（ＤＮＫ：Device Node Key）は、コンテンツの利用を正当なコンテンツ利用権を有するユーザデバイスにおいてのみ暗号化コンテンツを復号して利用可能とするためのコンテンツ利用に必要となる暗号鍵を取得するための鍵データである。

ＥＫＢ，ＤＮＫについては、後段で説明する。

【００４３】

コンテンツサーバ２３は、コンテンツを暗号化して、暗号化コンテンツをクライアント１０に提供する。さらに、ライセンスサーバ２２は、コンテンツ利用条件に基づいて利用権情報（Ｕｓａｇｅ Ｒｉｇｈｔ）を生成してユーザデバイス３０に提供する。さらに、管理システム３１の提供するデバイスノードキー（ＤＮＫ：Device Node Key）、有効化キーブロック（ＥＫＢ：Enabling Key Block）に基づいてサービスデータを生成してクライアント１０に提供する。サービスデータは、暗号化コンテンツの復号処理の際に必要となるサービス・デバイスノードキー（ＳＤＮＫ）を持つ有効化キーブロック（ＥＫＢ）を含む。

【００４４】

なお、コンテンツの利用条件には、利用期間の限定条件、コピーの回数制限、さらにコンテンツを同時に利用することができるポータブルメディア（ＰＭ：Portable Media）の数（いわゆるチェックアウト（Check-out）数に対応）の制限等がある。ポータブルメディア（ＰＭ：Portable Media）は例えばフラッシュメモリ、または小型ＨＤ、光ディスク、光磁気ディスク、ＭＤ（Mini Disk)等、ポータブルデバイスにおいて利用可能な記憶媒体である。

【００４５】

次に、図２を参照して、クライアント１０、ショップサーバ２１、ライセンスサーバ２２、コンテンツサーバ２３、管理システム３１として機能可能な情報処理装置の構成例を示す。これらの各システムはＣＰＵを持つ例えばＰＣ、サーバ等のシステムにそれぞれの処理に応じた処理プログラムを格納することで実現される。

【００４６】

まず、図２を用いて各システムの構成例について説明する。ＣＰＵ（Central Processing Unit）１０１は、ＲＯＭ（Read Only Memory）１０２に記憶されている各種プログラム、あるいは、記憶部１０８に格納され、ＲＡＭ（Random Access Memory）１０３にロードされたプログラムに従って各種処理を実行する。タイマ１００は計時処理を行ない、クロック情報をＣＰＵ１０１に供給する。

【００４７】

ＲＯＭ（Read Only Memory）１０２は、ＣＰＵ１０１が使用するプログラムや演算用のパラメータ、固定データ等を格納する。ＲＡＭ（Random Access Memory）１０３は、ＣＰＵ１０１の実行において使用するプログラムや、その実行において適宜変化するパラメータ等を格納する。これら各素子はＣＰＵバスなどから構成されるバス１１１により相互に接続されている。

【００４８】

暗号化復号部１０４は、コンテンツの暗号化、復号処理、デバイスノードキー（ＤＮＫ：Device Node Key）、有効化キーブロック（ＥＫＢ：Enabling Key Block）の適用処理として、例えばＤＥＳ(Data Encryption Standard)の暗号化アルゴリズムを適用した暗号処理、ＭＡＣ生成、検証処理等を実行する。さらに、他の接続装置との間で実行されるコンテンツあるいはライセンス情報の送受信時の認証およびセッションキー共有処理等、各種暗号処理を実行する。

【００４９】

コーデック部１０５は、例えばＡＴＲＡＣ(Adaptive Transform Acoustic Coding)３方式、ＭＰＥＧ、ＪＰＥＧ方式等、各種方式のデータエンコード処理、デコード処理を実行する。処理対象データは、バス１１１、入出力インタフェース１１２、ドライブ１１０を介してリムーバブル記憶媒体１２１からまたは通信部１０９を介して入力する。また処理後のデータは、必要に応じて、リムーバブル記憶媒体１２１に格納し、または通信部１０９を介して出力する。

【００５０】

入出力インタフェース１１２には、キーボード、マウス等の入力部１０６、ＣＲＴ、ＬＣＤ等のディスプレイ、スピーカ等からなる出力部１０７、ハードディスク等の記憶部１０８、モデム、ターミナルアダプタ等によって構成される通信部１０９が接続され、例えばインターネット等の通信網を介したデータ送受信を行なう。

【００５１】

［２．キー配信構成としてのツリー（木）構造について］

次に、正当なコンテンツ利用権を有するクライアントにおいてのみコンテンツ

を利用可能とするための、ブロードキャストエンクリプション（Broadcast Encryption）方式の一態様であるツリー構成によるデバイスとキーの管理構成について説明する。

【００５２】

図３の最下段に示すナンバ０～１５がコンテンツ利用を行なうクライアントとしてのユーザデバイスである。すなわち図３に示す階層ツリー（木）構造の各葉(リーフ：leaf)がそれぞれのデバイスに相当する。

【００５３】

各デバイス０～１５は、製造時あるいは出荷時、あるいはその後において、図３に示す階層ツリー（木）構造における自分のリーフからルートに至るまでのノードに割り当てられた鍵（ノードキー）および各リーフのリーフキーからなるキーセット（デバイスノードキー（ＤＮＫ：Device Node Key））をメモリに格納する。図３の最下段に示すＫ０００００～Ｋ１１１１が各デバイス０～１５にそれぞれ割り当てられたリーフキーであり、最上段のＫＲ（ルートキー）から、最下段から２番目の節（ノード）に記載されたキー：ＫＲ～Ｋ１１１をノードキーとする。

【００５４】

図３に示すツリー構成において、例えばデバイス０はリーフキーＫ００００と、ノードキー：Ｋ０００、Ｋ００、Ｋ０、ＫＲを所有する。デバイス５はＫ０１０１、Ｋ０１０、Ｋ０１、Ｋ０、ＫＲを所有する。デバイス１５は、Ｋ１１１１、Ｋ１１１、Ｋ１１、Ｋ１、ＫＲを所有する。なお、図３のツリーにはデバイスが０～１５の１６個のみ記載され、ツリー構造も４段構成の均衡のとれた左右対称構成として示しているが、さらに多くのデバイスがツリー中に構成され、また、ツリーの各部において異なる段数構成を持つことが可能である。

【００５５】

また、図３のツリー構造に含まれる各デバイスには、様々な記録媒体、例えば、デバイス埋め込み型あるいはデバイスに着脱自在に構成されたＤＶＤ、ＣＤ、ＭＤ、フラッシュメモリ等を使用する様々なタイプのデバイスが含まれている。さらに、様々なアプリケーションサービスが共存可能である。このような異なる

デバイス、異なるアプリケーションの共存構成の上に図３に示すコンテンツあるいは鍵配布構成である階層ツリー構造が適用される。

【００５６】

これらの様々なデバイス、アプリケーションが共存するシステムにおいて、例えば図３の点線で囲んだ部分、すなわちデバイス０，１，２，３を同一の記録媒体を用いる１つのグループとして設定する。例えば、この点線で囲んだグループ内に含まれるデバイスに対しては、まとめて、共通のコンテンツを暗号化してプロバイダから送付したり、各デバイス共通に使用するコンテンツキーを送付したり、あるいは各デバイスからプロバイダあるいは決済機関等にコンテンツ料金の支払データをやはり暗号化して出力するといった処理が実行される。コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等、各デバイスとのデータ送受信を行なう機関は、図３の点線で囲んだ部分、すなわちデバイス０，１，２，３を１つのグループとして一括してデータを送付する処理を実行する。このようなグループは、図３のツリー中に複数存在する。コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等、各デバイスとのデータ送受信を行なう機関は、メッセージデータ配信手段として機能する。

【００５７】

なお、ノードキー、リーフキーは、ある１つの鍵管理センター機能を持つ管理システムによって統括して管理してもよいし、各グループに対する様々なデータ送受信を行なうプロバイダ、決済機関等のメッセージデータ配信手段によってグループごとに管理する構成としてもよい。これらのノードキー、リーフキーは例えばキーの漏洩等の場合に更新処理が実行され、この更新処理は鍵管理センター機能を持つ管理システム、プロバイダ、決済機関等が実行する。

【００５８】

このツリー構造において、図３から明らかなように、１つのグループに含まれる３つのデバイス０，１，２，３はデバイスノードキー（ＤＮＫ：Device Node Key）として共通のキーＫ００、Ｋ０、ＫＲを含むデバイスノードキー（ＤＮＫ：Device Node Key）を保有する。このノードキー共有構成を利用することにより、例えば共通のキーをデバイス０，１，２，３のみに提供することが可能とな

る。たとえば、共通に保有するノードキーＫ００は、デバイス０，１，２，３に共通する保有キーとなる。また、新たなキーＫｎｅｗをノードキーＫ００で暗号化した値Ｅｎｃ（Ｋ００，Ｋｎｅｗ）を、ネットワークを介してあるいは記録媒体に格納してデバイス０，１，２，３に配布すれば、デバイス０，１，２，３のみが、それぞれのデバイスにおいて保有する共有ノードキーＫ００を用いて暗号Ｅｎｃ（Ｋ００，Ｋｎｅｗ）を解いて新たなキーＫｎｅｗを得ることが可能となる。なお、Ｅｎｃ（Ｋａ，Ｋｂ）はＫｂをＫａによって暗号化したデータであることを示す。

【００５９】

また、ある時点ｔにおいて、デバイス３の所有する鍵：Ｋ００１１,Ｋ００１，Ｋ００,Ｋ０,ＫＲが攻撃者（ハッカー）により解析されて露呈したことが発覚した場合、それ以降、システム（デバイス０，１，２，３のグループ）で送受信されるデータを守るために、デバイス３をシステムから切り離す必要がある。そのためには、ノードキー：Ｋ００１,Ｋ００,Ｋ０,ＫＲをそれぞれ新たな鍵Ｋ（ｔ）００１,Ｋ（ｔ）００,Ｋ（ｔ）０,Ｋ（ｔ）Ｒに更新し、デバイス０，１，２にその更新キーを伝える必要がある。ここで、Ｋ（ｔ）ａａａは、鍵Ｋａａａの世代（Generation）：ｔの更新キーであることを示す。

【００６０】

更新キーの配布処理ついて説明する。キーの更新は、例えば、図４（Ａ）に示す有効化キーブロック（ＥＫＢ：Enabling Key Block）と呼ばれるブロックデータによって構成されるテーブルをたとえばネットワーク、あるいは記録媒体に格納してデバイス０，１，２に供給することによって実行される。なお、有効化キーブロック（ＥＫＢ）は、図３に示すようなツリー構造を構成する各リーフに対応するデバイスに新たに更新されたキーを配布するための暗号化キーによって構成される。有効化キーブロック（ＥＫＢ）は、キー更新ブロック（ＫＲＢ：Key Renewal Block）と呼ばれることもある。

【００６１】

図４（Ａ）に示す有効化キーブロック（ＥＫＢ）には、ノードキーの更新の必要なデバイスのみが更新可能なデータ構成を持つブロックデータとして構成され

る。図４の例は、図３に示すツリー構造中のデバイス０，１，２において、世代ｔの更新ノードキーを配布することを目的として形成されたブロックデータである。図３から明らかなように、デバイス０，デバイス１は、更新ノードキーとしてＫ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要であり、デバイス２は、更新ノードキーとしてＫ（ｔ）００１、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒが必要である。

【００６２】

図４（Ａ）のＥＫＢに示されるようにＥＫＢには複数の暗号化キーが含まれる。最下段の暗号化キーは、Ｅｎｃ（Ｋ００１０，Ｋ（ｔ）００１）である。これはデバイス２の持つリーフキーＫ００１０によって暗号化された更新ノードキーＫ（ｔ）００１であり、デバイス２は、自身の持つリーフキーによってこの暗号化キーを復号し、Ｋ（ｔ）００１を得ることができる。また、復号により得たＫ（ｔ）００１を用いて、図４（Ａ）の下から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００１，Ｋ（ｔ）００）を復号可能となり、更新ノードキーＫ（ｔ）００を得ることができる。以下順次、図４（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図４（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。一方、デバイスＫ００００．Ｋ０００１は、ノードキーＫ０００は更新する対象に含まれておらず、更新ノードキーとして必要なのは、Ｋ（ｔ）００、Ｋ（ｔ）０、Ｋ（ｔ）Ｒである。デバイスＫ００００．Ｋ０００１は、図４（Ａ）の上から３段目の暗号化キーＥｎｃ（Ｋ０００，Ｋ（ｔ）００）を復号しＫ（ｔ）００、を取得し、以下、図４（Ａ）の上から２段目の暗号化キーＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）を復号し、更新ノードキーＫ（ｔ）０、図４（Ａ）の上から１段目の暗号化キーＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）を復号しＫ（ｔ）Ｒを得る。このようにして、デバイス０，１，２は更新した鍵Ｋ（ｔ）Ｒを得ることができる。なお、図４（Ａ）のインデックスは、復号キーとして使用するノードキー、リーフキーの絶対番地を示す。

【００６３】

図３に示すツリー構造の上位段のノードキー：Ｋ（ｔ）０,Ｋ（ｔ）Ｒの更新

が不要であり、ノードキーＫ００のみの更新処理が必要である場合には、図４（Ｂ）の有効化キーブロック（ＥＫＢ）を用いることで、更新ノードキーＫ（ｔ）００をデバイス０，１，２に配布することができる。

【００６４】

図４（Ｂ）に示すＥＫＢは、例えば特定のグループにおいて共有する新たなコンテンツキーを配布する場合に利用可能である。具体例として、図３に点線で示すグループ内のデバイス０，１，２，３がある記録媒体を用いており、新たな共通のコンテンツキーＫ（ｔ）ｃｏｎが必要であるとする。このとき、デバイス０，１，２，３の共通のノードキーＫ００を更新したＫ（ｔ）００を用いて新たな共通の更新コンテンツキー：Ｋ（ｔ）ｃｏｎを暗号化したデータＥｎｃ（Ｋ（ｔ），Ｋ（ｔ）ｃｏｎ）を図４（Ｂ）に示すＥＫＢとともに配布する。この配布により、デバイス４など、その他のグループの機器においては復号されないデータとしての配布が可能となる。

【００６５】

すなわち、デバイス０，１，２はＥＫＢを処理して得たＫ（ｔ）００を用いて上記暗号文を復号すれば、ｔ時点でのキー、例えばコンテンツの暗号化復号化に適用するコンテンツキーＫ（ｔ）ｃｏｎを得ることが可能になる。

【００６６】

［３．ＥＫＢを使用したキーの配布］

図５に、ｔ時点でのキー、例えばコンテンツの暗号化復号化に適用するコンテンツキーＫ（ｔ）ｃｏｎを得る処理例として、Ｋ（ｔ）００を用いて新たな共通のコンテンツキーＫ（ｔ）ｃｏｎを暗号化したデータＥｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）ｃｏｎ）と図４（Ｂ）に示すＥＫＢとを記録媒体を介して受領したデバイス０の処理例を示す。すなわちＥＫＢによる暗号化メッセージデータをコンテンツキーＫ（ｔ）ｃｏｎとした例である。

【００６７】

図５に示すように、デバイス０は、記録媒体に格納されている世代：t時点のＥＫＢと自分があらかじめ格納しているノードキーＫ０００を用いて上述したと同様のＥＫＢ処理により、ノードキーＫ（ｔ）００を生成する。さらに、復号し

た更新ノードキーＫ（ｔ）００を用いて更新コンテンツキーＫ（ｔ）ｃｏｎを復号して、後にそれを使用するために自分だけが持つリーフキーＫ００００で暗号化して格納する。

【００６８】

［４．ＥＫＢのフォーマット］

図６に有効化キーブロック（ＥＫＢ）のフォーマット例を示す。バージョン２０１は、有効化キーブロック（ＥＫＢ）のバージョンを示す識別子である。なお、バージョンは最新のＥＫＢを識別する機能とコンテンツとの対応関係を示す機能を持つ。デプスは、有効化キーブロック（ＥＫＢ）の配布先のデバイスに対する階層ツリーの階層数を示す。データポインタ２０３は、有効化キーブロック（ＥＫＢ）中のデータ部の位置を示すポインタであり、タグポインタ２０４はタグ部の位置、署名ポインタ２０５は署名の位置を示すポインタである。

【００６９】

データ部２０６は、例えば更新するノードキーを暗号化したデータを格納する。例えば図５に示すような更新されたノードキーに関する各暗号化キー等を格納する。

【００７０】

タグ部２０７は、データ部に格納された暗号化されたノードキー、リーフキーの位置関係を示すタグである。このタグの付与ルールを図７を用いて説明する。図７では、データとして先に図４（Ａ）で説明した有効化キーブロック（ＥＫＢ）を送付する例を示している。この時のデータは、図７の表（ｂ）に示すようになる。このときの暗号化キーに含まれるトップノードのアドレスをトップノードアドレスとする。この場合は、ルートキーの更新キーＫ（ｔ）Ｒが含まれているので、トップノードアドレスはＫＲとなる。このとき、例えば最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）は、図７の（ａ）に示す階層ツリーに示す位置にある。ここで、次のデータは、Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）であり、ツリー上では前のデータの左下の位置にある。データがある場合は、タグが０、ない場合は１が設定される。タグは｛左（Ｌ）タグ，右（Ｒ）タグ｝として設定される。最上段のデータＥｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）Ｒ）の左にはデータがあ

るので、Ｌタグ＝０、右にはデータがないので、Ｒタグ＝１となる。以下、すべてのデータにタグが設定され、図７（ｃ）に示すデータ列、およびタグ列が構成される。

【００７１】

タグは、データＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）がツリー構造のどこに位置しているのかを示すために設定されるものである。データ部に格納されるキーデータＥｎｃ（Ｋｘｘｘ，Ｋｙｙｙ）．．．は、単純に暗号化されたキーの羅列データに過ぎないので、上述したタグによってデータとして格納された暗号化キーのツリー上の位置を判別可能としたものである。上述したタグを用いずに、先の図４で説明した構成のように暗号化データに対応させたノード・インデックスを用いて、例えば、

０：Ｅｎｃ（Ｋ（ｔ）０，Ｋ（ｔ）ｒｏｏｔ）

００：Ｅｎｃ（Ｋ（ｔ）００，Ｋ（ｔ）０）

０００：Ｅｎｃ（Ｋ（（ｔ）０００，Ｋ（Ｔ）００）

．．．のようなデータ構成とすることも可能であるが、このようなインデックスを用いた構成とすると冗長なデータとなりデータ量が増大し、ネットワークを介する配信等においては好ましくない。これに対し、上述したタグをキー位置を示す索引データとして用いることにより、少ないデータ量でキー位置の判別が可能となる。

【００７２】

図６に戻って、ＥＫＢフォーマットについてさらに説明する。署名（Signature）２０８は、有効化キーブロック（ＥＫＢ）を発行した例えば鍵管理センター機能を持つ管理システム、コンテンツサーバ、ライセンスサーバ、あるいはショップサーバ等が実行する電子署名である。ＥＫＢを受領したデバイスは署名検証によって正当な有効化キーブロック（ＥＫＢ）発行者が発行した有効化キーブロック（ＥＫＢ）であることを確認する。

【００７３】

［５．ツリーのカテゴリ分類］

ノードキー等を定義している階層ツリー構造を各デバイスのカテゴリ毎に分類

して効率的なキー更新処理、暗号化キー配信、データ配信を実行する構成について、以下説明する。

【００７４】

図８に階層ツリー構造のカテゴリの分類の一例を示す。図８において、階層ツリー構造の最上段には、ルートキーＫｒｏｏｔ３０１が設定され、以下の中間段にはノードキー３０２が設定され、最下段には、リーフキー３０３が設定される。各デバイスは個々のリーフキーと、リーフキーからルートキーに至る一連のノードキー、ルートキーを保有する。

【００７５】

ここで、一例として最上段から第M段目のあるノードをカテゴリノード３０４として設定する。すなわち第M段目のノードの各々を特定カテゴリのデバイス設定ノードとする。第M段の１つのノードを頂点として以下、Ｍ＋１段以下のノード、リーフは、そのカテゴリに含まれるデバイスに関するノードおよびリーフとする。

【００７６】

例えば図８の第M段目の１つのノード３０５にはカテゴリ［メモリステッイク（商標）］が設定され、このノード以下に連なるノード、リーフはメモリステッイクを使用した様々なデバイスを含むカテゴリ専用のノードまたはリーフとして設定される。すなわち、ノード３０５以下を、メモリスティックのカテゴリに定義されるデバイスの関連ノード、およびリーフの集合として定義する。

【００７７】

さらに、M段から数段分下位の段をサブカテゴリノード３０６として設定することができる。例えば図に示すようにカテゴリ［メモリスティック］ノード３０５の２段下のノードに、メモリスティックを使用したデバイスのカテゴリに含まれるサブカテゴリノードとして、［再生専用器］のノードを設定する。さらに、サブカテゴリノードである再生専用器のノード３０６以下に、再生専用器のカテゴリに含まれる音楽再生機能付き電話のノード３０７が設定され、さらにその下位に、音楽再生機能付き電話のカテゴリに含まれる［ＰＨＳ］ノード３０８と［携帯電話］ノード３０９を設定することができる。

【００７８】

さらに、カテゴリ、サブカテゴリは、デバイスの種類のみならず、例えばあるメーカー、コンテンツプロバイダ、決済機関等が独自に管理するノード、すなわち処理単位、管轄単位、あるいは提供サービス単位等、任意の単位（これらを総称して以下、エンティティと呼ぶ）で設定することが可能である。例えば１つのカテゴリノードをゲーム機器メーカーの販売するゲーム機器ＸＹＺ専用の頂点ノードとして設定すれば、メーカーの販売するゲーム機器ＸＹＺにその頂点ノード以下の下段のノードキー、リーフキーを格納して販売することが可能となり、その後、暗号化コンテンツの配信、あるいは各種キーの配信、更新処理を、その頂点ノードキー以下のノードキー、リーフキーによって構成される有効化キーブロック（ＥＫＢ）を生成して配信し、頂点ノード以下のデバイスに対してのみ利用可能なデータが配信可能となる。

【００７９】

このように、１つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定する構成とすることにより、カテゴリ段、あるいはサブカテゴリ段の１つの頂点ノードを管理するメーカー、コンテンツプロバイダ等がそのノードを頂点とする有効化キーブロック（ＥＫＢ）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が可能となり、頂点ノードに属さない他のカテゴリのノードに属するデバイスには全く影響を及ぼさずにキー更新を実行することができる。

【００８０】

本発明のシステムにおいては、図９に示されるように、ツリー構成のシステムで、キーの管理が行われる。図９の例では、８＋２４＋３２段のノードがツリー構造とされ、ルートノードから下位の８段までの各ノードにカテゴリが対応される。ここにおけるカテゴリとは、例えばメモリスティックなどの半導体メモリを使用する機器のカテゴリ、デジタル放送を受信する機器のカテゴリといったカテゴリを意味する。そして、このカテゴリノードのうちの１つのノードに、ライセンスを管理するシステムとして本システム（Ｔシステムと称する）が対応する。

【００８１】

すなわち、このＴシステムのノードよりさらに下の階層の２４段のノードに対応するキーが、サービスプロバイダ、あるいはサービスプロバイダが提供するサービスに適用される。この例の場合、これにより、2^{24}（約１６メガ）のサービスプロバイダあるいはサービスを規定することができる。さらに、最も下側の３２段の階層により、2^{32}（約４ギガ）のユーザ（あるいはユーザデバイス）を規定することができる。最下段の３２段のノードからＴシステムのノードまでのパス上の各ノードに対応するキーが、ＤＮＫ（Device Node Key）を構成し、最下段のリーフに対応するＩＤがリーフＩＤとされる。

【００８２】

例えば、コンテンツを暗号化したコンテンツキーは更新されたルートキーＫＲ’によって暗号化され、上位の階層の更新ノードキーは、その直近の下位の階層の更新ノードキーを用いて暗号化され、ＥＫＢ内に配置される。ＥＫＢにおける末端から１つ上の段の更新ノードキーはＥＫＢの末端のノードキーあるいはリーフキーによって暗号化され、ＥＫＢ内に配置される。

【００８３】

ユーザデバイスは、サービスデータに記述されているＤＮＫのいずれかのキーを用いて、コンテンツデータとともに配布されるＥＫＢ内に記述されている直近の上位の階層の更新ノードキーを復号し、復号して得たキーを用いて、ＥＫＢ内に記述されているさらにその上の階層の更新ノードキーを復号する。以上の処理を順次行うことで、ユーザデバイスは、更新ルートキーＫＲ’を得ることができる。

【００８４】

上述したように、ツリーのカテゴリ分類により、１つのノードを頂点として、以下のノードをその頂点ノードに定義されたカテゴリ、あるいはサブカテゴリの関連ノードとして設定した構成が可能となり、カテゴリ段、あるいはサブカテゴリ段の１つの頂点ノードを管理するメーカー、サービスプロバイダ等がそのノードを頂点とする有効化キーブロック（ＥＫＢ）を独自に生成して、頂点ノード以下に属するデバイスに配信する構成が実現される。

【００８５】

さらに、上述のツリー構成のデバイス管理によるＥＫＢ配信システムを適用して、複数のカテゴリに基づくＥＫＢ配信構成を採用したコンテンツ配信および利用形態について説明する。

【００８６】

図１０を参照して２つのカテゴリについて説明する。図１０に示すように、ルートノード３５０の下段にＴシステムノード３５１を設定し、その下段にＴサービスノード３５２、およびＴハードノード３５３を設定する。Ｔハードノード３５３を頂点としたツリーは、ユーザデバイス機器自体をリーフ３５５として設定し、機器を対象として発行するハード対応ＥＫＢ［ＥＫＢ（Ｈ）］を配信するカテゴリツリーである。一方、Ｔサービスノード３５２を頂点としたツリーは、ユーザデバイス機器に提供するサービスに対応して発行するサービス対応ＥＫＢ［ＥＫＢ（Ｓ）］を配信するカテゴリツリーである。

【００８７】

ハード対応ＥＫＢ［ＥＫＢ（Ｈ）］、サービス対応ＥＫＢ［ＥＫＢ（Ｓ）］とも、それぞれ正当な権限を持つデバイスに対して与えられるＤＮＫ（Device Node Key）すなわち、リーフからＴシステムのノードまでのパス上の各ノードに対応するキーを有することで、各ＥＫＢの復号が可能となる。

【００８８】

［６．コンテンツ購入および試聴処理］

次に、クライアントがコンテンツを購入または試聴する際の処理の詳細について、図１１以下を参照して説明する。

【００８９】

図１１は、クライアントアプリケーション、ブラウザを有するＰＣ等のクライアントと、ショップサーバ、コンテンツサーバ、ライセンスサーバ、および管理システムとの間で実行されるコンテンツ購入処理における通信シーケンスの初期ステップを示している。以下、シーケンス図に示す処理について説明する。

【００９０】

まず、クライアント側において、コンテンツの購入を行なおうとするユーザは、自己のＰＣ等の通信可能な情報処理装置にＵＲＬを指定（ステップ（１））し

、ブラウザが介してショップサーバの提示するコンテンツリスト画面（ショップページ）を読み出し（ステップ（２））て、ディスプレイに表示（ステップ（３））する。

【００９１】

クライアントは、ショップサーバの提示するコンテンツリストからコンテンツを選択して、さらに、購入または試聴どちらかの指定（ステップ（４））を行なって、ブラウザを介してショップサーバに要求データを送信（ステップ（５））する。要求データには、コンテンツＩＤ（ＣＩＤ）、ショップサーバ識別子（ＳｈｏｐＩＤ）、および購入または試聴どちらかの指定データが含まれる。

【００９２】

ショップサーバは、クライアントからのコンテンツ購入、または試聴要求を受信すると、管理システムに対して、コンテンツの提供の可否判定を要求（ステップ（６））する。この判定要求には、コンテンツＩＤ（ＣＩＤ）、ショップサーバ識別子（ＳｈｏｐＩＤ）が含まれる。

【００９３】

管理システムは、コンテンツの提供の可否判定要求を受信すると、トランザクションＩＤ（ＴＩＤ）の発行処理（ステップ（７））を実行する。トランザクションＩＤ（ＴＩＤ）の発行処理の詳細を図１２のフローを参照して説明する。

【００９４】

管理システムは、まず、ステップＳ１０１において、乱数を発生し、発生乱数に基づいて、トランザクションＩＤ（ＴＩＤ）を生成する。次に、ステップＳ１０２において、生成したトランザクションＩＤ（ＴＩＤ）と、ショップサーバから指定されたコンテンツＩＤ（ＣＩＤ）とを対応付けてトランザクションデータとして記憶部に格納する。次に、生成したトランザクションＩＤ（ＴＩＤ）をショップサーバに対して出力、発行する。

【００９５】

図１１のシーケンス図に戻る。管理システムは、トランザクションＩＤ（ＴＩＤ）の生成後、生成したトランザクションＩＤ（ＴＩＤ）と価格情報をＴＩＤ情報としてショップサーバに送信（ステップ（８））する。ただし、価格情報は、

コンテンツ購入時においてのみ要求される情報であり、コンテンツ試聴処理に際しては、含まれない。ＴＩＤ情報を受信したショップサーバは、クライアントからの要求がコンテンツ購入である場合に、ＴＩＤ情報に含まれる価格に基づいて、課金処理（ステップ（９））を実行する。

【００９６】

クライアントからの要求がコンテンツ購入ではなく、コンテンツ試聴要求である場合には、この課金処理（ステップ（９））は省略される。

【００９７】

次に、図１３のシーケンス図を参照して継続する処理について説明する。ショップサーバは、コンテンツ購入処理においては、課金が実行されたことを条件として、またコンテンツ試聴処理においては、管理システムからのＴＩＤ情報の受信を条件として、購入または試聴要求対象のコンテンツのダウンロード許可要求を管理システムに対して送信（ステップ（１０））する。

【００９８】

管理システムは、ダウンロード許可要求を受信すると、ダウンロード許可要求検証処理（ステップ（１１））を実行する。ダウンロード許可要求検証処理の詳細を図１４のフローを参照して説明する。

【００９９】

管理システムは、まず、ステップＳ２０１において、受信したダウンロード許可要求に含まれるトランザクションＩＤ（ＴＩＤ）と、先に生成し、記憶部に格納したトランザクションＩＤ（ＴＩＤ）とを照合し、さらにステップＳ２０２において、照合の成立したトランザクションＩＤ（ＴＩＤ）に対応して記録されたコンテンツＩＤ（ＣＩＤ）を取得し、ステップＳ２０３において、ＣＩＤに対応するコンテンツのダウンロード許可を発行する。

【０１００】

図１３のシーケンス図に戻り、説明を続ける。管理システムは、ダウンロード許可要求検証処理（ステップ（１１））の後、コンテンツのダウンロード許可をショップサーバに対して発行（ステップ（１２））する。ダウンロード許可には、トランザクションＩＤ（ＴＩＤ）、コンテンツサーバＵＲＬ（Ｃ－ＵＲＬ）、

ライセンスサーバＵＲＬ（Ｌ－ＵＲＬ）、コンテンツＩＤ（ＣＩＤ）、利用権情報ＩＤ（ＵＩＤ）、商品（コンテンツ）ＵＲＬ（Ｓ－ＵＲＬ）、サービスＩＤが含まれる。

【０１０１】

ショップサーバは、管理システムからダウンロード許可を受信すると、クライアントアプリケーションにおけるコンテンツの利用（再生処理等）プログラムを起動させるための起動ファイルを生成してクライアントのブラウザを介してクライアントアプリケーションに対して送付する。

【０１０２】

起動ファイルの例を図１５を参照して説明する。起動ファイル３６０は、先に管理システムが生成したトランザクションＩＤ（ＴＩＤ）、クライアントが購入あるいは試聴するコンテンツＩＤ（ＣＩＤ）、管理システムが生成したダウンロード許可情報に含まれる利用権情報ＩＤ（ＵＩＤ）、管理システムが生成したダウンロード許可情報に含まれるサービスＩＤ、ライセンスサーバＵＲＬ、商品（コンテンツ）ＵＲＬ、さらに、処理が購入であるか試聴であるかの識別データが含まれる。

【０１０３】

なお、処理が購入であるか試聴であるかの識別データとしては、起動ファイルに設定される拡張子を購入であるか試聴であるかによって区別して設定し、これをクライアントアプリケーションが判別して、それぞれのアプリケーションを起動するようにしてもよい。

【０１０４】

クライアントアプリケーションは、起動ファイルに応じて、アプリケーションを起動（ステップ（１５））する。

【０１０５】

クライアントアプリケーションにおいて実行するアプリケーション起動処理について、図１６を参照して説明する。ステップＳ３０１において、まず、起動ファイルに設定されたサービスＩＤ対応のサービスデータをクライアントシステムとしての情報処理装置に格納されているか否かを判定する。

【０１０６】

サービスデータは、クライアントが各種のサービス、例えばコンテンツ利用サービスを受領したい場合、ライセンスサーバから受領するもので、例えば特定のサービスプロバイダの提供サービスの一括したサービス利用権を認めるデータである。図１７（ａ）にサービスデータのデータ構成例を示す。

【０１０７】

図１７（ａ）に示すように、サービスデータ３７０には、ＥＫＢ配信ツリーにおいて設定されるクライアントに固有のリーフＩＤ、サービス識別子としてのサービスＩＤ、さらにデバイスノードキー（ＤＮＫ）をルートキー（Ｋｒｏｏｔ）で暗号化したデータ、Ｅ（Ｋｒｏｏｔ，ＤＮＫ）が含まれる。サービスデータを受領するためには、クライアントは、ライセンスサーバに対する登録処理が必要とされる。登録処理は、図１３に示す処理ステップ（１５）、（１６）の処理に対応する。

【０１０８】

図１６に示すステップＳ３０１において、サービスＩＤ対応のサービスデータを保有していないと判定すると、ステップＳ３０２において登録処理を実行して、サービスデータを受領する。

【０１０９】

さらに、この登録処理時に、デフォルト利用権情報がライセンスサーバからクライアントに対して発行される。利用権情報は、通常は、購入コンテンツの利用条件を格納し、コンテンツの購入に対応して発行されるものであるが、デフォルト利用権情報は、コンテンツの購入を条件として発行するものではなく、クライアントの登録処理、あるいはサービスデータの発行処理を条件として発行する。このデフォルト利用権情報は、後段で説明するコンテンツの試聴処理の際の有効なコンテンツ利用権情報として適用される。

【０１１０】

図１７（ｂ）に利用権情報のデータ構成例を示す。図１７（ｂ）に示すように、利用権情報３７１には、利用権情報識別子としての利用権情報ＩＤ、発行日時情報としてのタイムスタンプ、クライアントに固有のリーフＩＤ、コンテンツ対

応である場合は、コンテンツＩＤ、さらに、利用条件対象コンテンツ種別情報が格納される。

【０１１１】

デフォルト利用権情報の場合は、特定の購入コンテンツに対応して発行されるものではないため、コンテンツＩＤは省略、あるいは試聴可能なコンテンツに共通なＩＤが設定される。また、利用条件対象コンテンツ種別情報として、例えば試聴フラグがオン（ＯＮ）として設定されたコンテンツについての利用が許可される設定とする。コンテンツ３７２には図１７（ｃ）に示すように、試聴フラグ３７３が設定され、試聴フラグ３７３がオン（ＯＮ）の設定コンテンツであれば、試聴が許可されたコンテンツであることを示し、試聴フラグがオフ（ＯＦＦ）の設定コンテンツであれば、試聴が許可されていないコンテンツであることを示す。

【０１１２】

クライアントアプリケーションは、試聴コンテンツ再生時には、デフォルト利用権情報を参照して、再生許可の有無を判定するとともに、コンテンツのフラグの検証を実行して、コンテンツの再生を行なうことになる。この処理については、後段で説明する。

【０１１３】

図１６の処理フローに戻りアプリケーション起動処理の処理手順について説明する。ステップＳ３０２において、登録処理、すなわちライセンスサーバからのサービスデータ、デフォルト利用権情報の取得が終了すると、ステップＳ３０３において、ショップサーバから受信した起動ファイルが、購入用アプリケーションの起動ファイルであるか、試聴用アプリケーションの起動ファイルであるかを判別する。購入用アプリケーションの起動ファイルである場合は、ステップＳ３０４に進み購入用アプリケーションを実行し、試聴用アプリケーションの起動ファイルである場合は、ステップＳ３０５に進み試聴用アプリケーションを実行する。

【０１１４】

次に、購入用アプリケーションの実行シーケンスについて、図１８のシーケン

ス図を参照して説明する。

【０１１５】

購入処理実行の場合、クライアントアプリケーションは、コンテンツダウンロード要求をコンテンツサーバに対して実行（ステップ（２１））する。これは、先にクライアントが購入要求を行なったコンテンツであり、利用権情報（図１７（ｂ）参照）に記録されたコンテンツＩＤ（ＣＩＤ）に対応するコンテンツである。クライアントアプリケーションは、コンテンツＩＤ（ＣＩＤ）によりコンテンツを指定してコンテンツダウンロード要求をコンテンツサーバに対して実行する。

【０１１６】

コンテンツサーバは、コンテンツダウンロード要求を受信すると、ＣＩＤに対応するコンテンツ情報をクライアントに送信（ステップ（２２））する。このコンテンツ情報は、暗号化コンテンツを含み、図１７（ｃ）に示すように、コンテンツキー：Ｋｃで暗号化されたコンテンツデータ：Ｅｎｃ（Ｋｃ，Ｃｏｎｔｅｎｔ）、コンテンツキー：Ｋｃをルートキー：Ｋｒｏｏｔで暗号化したデータ：Ｅｎｃ（Ｋｒｏｏｔ，Ｋｃ）、さらに：ルートキー：Ｋｒｏｏｔを取得するためのＥＫＢ、さらに試聴フラグデータ、サービスＩＤ等の情報が付加されたファイルである。

【０１１７】

コンテンツ情報を受領したクライアントは、受信コンテンツに対応する利用権情報（Ｕｓａｇｅ　Ｒｉｇｈｔ）の取得要求をライセンスサーバに対して送信（ステップ（２３））する。この要求には、先にショップサーバから受領した起動ファイル（図１５参照）中に含まれる利用権情報ＩＤ（ＵＩＤ）、クライアント識別データとしてのリーフＩＤ、および先にショップサーバから受領した起動ファイル（図１５参照）中に含まれるトランザクションＩＤ（ＴＩＤ）が含まれる。

【０１１８】

ライセンスサーバは、利用権情報（Ｕｓａｇｅ　Ｒｉｇｈｔ）の取得要求を受信すると、管理システムに対して、注文照会処理（ステップ（２４））を行なう

。この要求には、利用権情報ＩＤ（ＵＩＤ）、トランザクションＩＤ（ＴＩＤ）が含まれる。注文照会を受信した管理サーバは、注文照会応答として、利用権情報ＩＤ（ＵＩＤ）に対応する利用条件を設定した応答情報をライセンスサーバに送信（ステップ（２５））する。

【０１１９】

応答情報を受信したライセンスサーバは、コンテンツ利用条件を設定した利用権情報（Ｕｓａｇｅ　Ｒｉｇｈｔ）を生成して、クライアントに対して発行（ステップ（２６））する。なお、コンテンツ利用条件とは、コンテンツの再生回数、期限、外部機器に対するコピー、チェツクアウト処理等の各種処理の許可情報によって構成される。

【０１２０】

利用権情報（Ｕｓａｇｅ　Ｒｉｇｈｔ）を受信したクライアントは、先にコンテンツサーバから受信したコンテンツについて、利用権情報（Ｕｓａｇｅ　Ｒｉｇｈｔ）に記録された利用条件に基づいてコンテンツの利用が可能となる。ユーザからコンテンツＩＤ（ＣＩＤ）、利用権情報（Ｕｓａｇｅ　Ｒｉｇｈｔ）ＩＤを指定したコンテンツ再生要求（ステップ（２７））があると、クライアントアプリケーションは、利用条件に従ったコンテンツ再生を実行（ステップ（２８））する。

【０１２１】

基本的なコンテンツ再生処理の手順について、図１９を参照して説明する。前述の説明から理解されるように、コンテンツサーバ３８２からクライアント３８３に対してコンテンツが提供されるとともに、ライセンスサーバ３８１からクライアント３８３にライセンスとして、サービスデータ、利用権情報（Ｕｓａｇｅ　Ｒｉｇｈｔ）が与えられる。

【０１２２】

コンテンツは、コンテンツキー：Ｋｃにより、暗号化されており（Ｅｎｃ（Ｋｃ，Ｃｏｎｔｅｎｔ）、コンテンツキーＫｃは、ＥＫＢから取得可能なルートキーＫｒｏｏｔから得られるキーである。

【０１２３】

クライアント３８３は、ライセンスサーバから受領したサービスデータからデバイスノードキー（ＤＮＫ）を取得し、取得したＤＮＫに基づいてコンテンツファイルのＥＫＢを復号して、ルートキー：Ｋｒｏｏｔを取得し、さらに、取得したルートキー：Ｋｒｏｏｔを用いて、Ｅｎｃ（Ｋｒｏｏｔ，Ｋｃ）を復号してコンテンツキー：Ｋｃを取得し、取得したコンテンツキー：Ｋｃをにより暗号化コンテンツ：Ｅｎｃ（Ｋｃ，Ｃｏｎｔｅｎｔ）の復号処理を実行してコンテンツを取得し、再生する。

【０１２４】

サービスデータ、利用権情報（Ｕｓａｇｅ　Ｒｉｇｈｔ）と対応付けたコンテンツ再生処理の詳細について、図２０を参照して説明する。

【０１２５】

図２０は、ハード対応ＥＫＢ［ＥＫＢ（Ｈ）］、サービス対応ＥＫＢ［ＥＫＢ（Ｓ）］を適用したコンテンツの復号処理に基づくコンテンツ利用処理シーケンスを説明した図である。

【０１２６】

図２０に示すサービスデータ４０１、および利用権情報４０３は、ライセンスサーバカラ受領するデータであり、暗号化コンテンツファイル４０２はコンテンツサーバから受領するデータである。サービスデータ４０１は、リーフ識別子としてのリーフＩＤ、適用するＥＫＢのバージョン、さらに、サービス対応ＥＫＢ［ＥＫＢ（Ｓ）］の復号に必要なサービス対応デバイスノードキー（ＳＤＮＫ）を、ハード対応カテゴリツリーに対応して設定されるルートキーＫｒｏｏｔ’によって暗号化したデータＥ（Ｋｒｏｏｔ’，ＳＤＮＫ）を格納している。

【０１２７】

暗号化コンテンツファイル４０２は、サービス対応のカテゴリツリーに対応して設定されるルートキーＫｒｏｏｔを格納したサービス対応ＥＫＢ［ＥＫＢ（Ｓ）］、ルートキーＫｒｏｏｔでコンテンツＩＤ（ＣＩＤ）と、コンテンツ暗号処理および復号処理に適用するコンテンツキー（Ｋｃ）とを暗号化したデータＥ（Ｋｒｏｏｔ，ＣＩＤ＋Ｋｃ）、および、コンテンツ（Ｃｏｎｔｅｎｔ）をコンテンツキーＫｃで暗号化したデータＥ（Ｋｃ，Ｃｏｎｔｅｔ）を含むファイルであ

る。

【０１２８】

また、利用権情報４０３は、リーフＩＤと、コンテンツの利用条件情報を格納したデータである。コンテンツの利用条件情報には、コンテンツに対応して設定される利用期間、利用回数、コピー制限等の様々な利用条件が含まれる。利用権情報４０３を受領したユーザデバイスは、利用権情報をコンテンツに対応するセキュリティ情報として格納するか、あるいは、コンテンツの索引データとしてのＡＶインデックスファイル内に格納する。

【０１２９】

例えば、ＰＣ等の大容量の記憶手段を有し、プロセッサ等の処理能力が高いユーザデバイスにおいては、利用権情報をコンテンツに対応するセキュリティ情報として格納することが可能であり、すべての利用権情報を格納して、コンテンツ利用の際にすべての利用権情報を参照した処理を行なうことが好ましい。一方、大容量の記憶手段を持たず、またプロセッサ等の処理能力が低いポータブルデバイス（ＰＤ）等のユーザデバイスにおいては、選択された情報からなる利用権情報４０３をコンテンツの索引データとしてのＡＶインデックスファイル内に格納して、コンテンツ利用の際にＡＶインデックスファイル内の利用条件情報を参照した処理を行なう等の処理が可能である。

【０１３０】

ユーザデバイスは、図２０に示すステップＳ５０１において、ハード対応のデバイスノードキー（ＨＤＮＫ）４１２を適用して、ハード対応のＥＫＢ（Ｈ）４１１の復号処理を実行し、ＥＫＢ（Ｈ）４１１から、ハード対応カテゴリツリーに対応して設定されるルートキーＫｒｏｏｔ’を取得する。ＤＮＫを適用したＥＫＢの処理は、先に図５を参照して説明した手法に従った処理となる。

【０１３１】

次に、ステップＳ５０２において、ＥＫＢ（Ｈ）から取り出したルートキーＫｒｏｏｔ’を用いて、サービスデータ４０１内の暗号化データＥ（Ｋｒｏｏｔ’，ＳＤＮＫ）の復号処理を実行し、サービス対応ＥＫＢ［ＥＫＢ（Ｓ）］の処理（復号）に適用するデバイスノードキー（ＳＤＮＫ）を取得する。

【０１３２】

次に、ステップＳ５０３において、サービスデータから取り出したデバイスノードキー（ＳＤＮＫ）を用いて、暗号化コンテンツファイル４０２内に格納されたサービス対応ＥＫＢ［ＥＫＢ（Ｓ）］の処理（復号）を実行し、サービス対応ＥＫＢ［ＥＫＢ（Ｓ）］内に格納されたサービス対応カテゴリツリーに対応して設定されるルートキーＫｒｏｏｔを取得する。

【０１３３】

次に、ステップＳ５０４において、サービス対応ＥＫＢ［ＥＫＢ（Ｓ）］から取り出したルートキーＫｒｏｏｔを用いて、暗号化コンテンツファイル４０２内に格納された暗号化データＥ（Ｋｒｏｏｔ，ＣＩＤ＋Ｋｃ）の復号処理を実行し、コンテンツＩＤ（ＣＩＤ）と、コンテンツキー（Ｋｃ）を取得する。

【０１３４】

次に、ステップＳ５０５において、暗号化コンテンツファイル４０２から取り出したコンテンツＩＤ（ＣＩＤ）と、利用権情報内に格納されたコンテンツＩＤのマッチング（照合）処理を実行する。マッチング処理により、コンテンツの利用が可能であることが確認されると、ステップＳ５０６において、暗号化コンテンツファイル４０２から取り出したコンテンツキー（Ｋｃ）を適用して、暗号化コンテンツファイル４０２に格納された暗号化コンテンツＥ（Ｋｃ，Ｃｏｎｔｅｎｔ）を復号してコンテンツの再生を行なう。

【０１３５】

上述したように、コンテンツ利用機器としてのハードウェアに対応して設定されたカテゴリツリーに対応するＥＫＢとしてのハード対応ＥＫＢ［ＥＫＢ（Ｈ）］と、コンテンツ利用サービスに対応して設定されたカテゴリツリーに対応するＥＫＢとしてのサービス対応ＥＫＢ［ＥＫＢ（Ｓ）］をそれぞれ個別にユーザに対して提供し、それぞれのＥＫＢに対する正当なＤＮＫを有するユーザのみがサービスの利用を行なうことが可能となる。

【０１３６】

サービス対応ＥＫＢ［ＥＫＢ（Ｓ）］を復号するためのＤＮＫ、すなわちＳＤＮＫは、コンテンツに対応したサービスデータ４０１として提供可能であり、ま

たＳＤＮＫを正当なハードウェア対応のＤＮＫ、すなわちＨＤＮＫを有する機器のみが取得可能なハード対応カテゴリツリーに対応して設定されるルートキーＫｒｏｏｔ’を適用して暗号化した構成としたので、正当なＨＤＮＫを有するユーザデバイスのみが、ＳＤＮＫを取得でき、サービスが利用となる。

【０１３７】

また、コンテンツ利用において、暗号化コンテンツファイル４０２から取得されるコンテンツ識別子（ＣＩＤ）と、利用権情報から取得されるＣＩＤとのマッチング処理を実行する構成としたので、利用権情報４０３を取得してＣＩＤ情報を格納していることがコンテンツ再生プロセスの必須用件とすることが可能となり、利用条件に従ったコンテンツ利用が実現される。

【０１３８】

次に、クライアントアプリケーションの処理が試聴処理の実行アプリケーションである場合の処理について、図２１のシーケンス図を参照して説明する。

【０１３９】

試聴処理の場合、コンテンツ購入処理と同様、コンテンツ情報ファイル（図１９参照）を取得してクライアントシステムの記憶部に格納し、その後、購入コンテンツと同様の処理によって再生することも可能であるが、記憶部に格納することなく、ストリーミング再生処理を実行する例について、図２１を参照して説明する。

【０１４０】

ストリーミング試聴処理実行の場合、クライアントアプリケーションは、コンテンツダウンロード要求をコンテンツサーバに対して実行（ステップ（３１））する。これは、先にクライアントが試聴要求を行なったコンテンツである。クライアントアプリケーションは、コンテンツＩＤ（ＣＩＤ）によりコンテンツを指定してコンテンツダウンロード要求をコンテンツサーバに対して実行する。

【０１４１】

コンテンツサーバは、ストリーミング再生の場合には、コンテンツの部分データ（コンテンツパート）を次々にクライアントに対して送信（ステップ（３２））する。コテンツパートを受信したクライアントは、受信コンテンツに対する再

生処理を実行（ステップ（３３））し、後続のコンテンツパートの要求をコンテンツサーバに送信する。この処理を連続して実行することによりストリーミング再生が行なわれる。

【０１４２】

試聴再生処理の手順について、図２２のフローを参照して説明する。ステップＳ７０１において、クライアントアプリケーションは、コンテンツサーバから受信した試聴コンテンツファイル中からサービスＩＤを取得する。

【０１４３】

次にステップＳ７０２において、抽出したサービスＩＤに対応するデフォルト利用権情報（Ｄｅｆａｕｌｔ　Ｕｓａｇｅ　Ｒｉｇｈｔ）（図１７（ｂ）参照）の有無を判定する。デフォルト利用権情報は、クライアントの登録処理時に、サービスデータ（図１７（ａ）参照）とともに、ライセンスサーバから送信される利用権情報であり、購入コンテンツに対応して発行される利用権情報と異なり、試聴可能なコンテンツに対して利用される利用権情報である。

【０１４４】

コンテンツ試聴においては、デフォルト利用権情報（Ｄｅｆａｕｌｔ　Ｕｓａｇｅ　Ｒｉｇｈｔ）を保有することが試聴実行許可条件であり、デフォルト利用権情報を保有していない場合は、ステップＳ７０５に進み、エラーとしてコンテンツ再生が実行されず処理を終了する。

【０１４５】

デフォルト利用権情報（Ｄｅｆａｕｌｔ　Ｕｓａｇｅ　Ｒｉｇｈｔ）が格納されている場合は、ステップＳ７０３において、デフォルト利用権情報を検証し、利用権情報の記録を確認する。デフォルト利用権情報には、例えば試聴フラグオンのコンテンツの試聴許可、あるいは試聴可能なコンテンツＩＤ情報が格納されており、これらの情報を取得する。

【０１４６】

次にステップＳ７０４において、デフォルト利用権情報（Ｄｅｆａｕｌｔ　Ｕｓａｇｅ　Ｒｉｇｈｔ）の利用条件に基づいてコンテンツが再生される。なお、再生処理は、前述の図１９、図２０を参照して説明したように、コンテンツサー

バから受信する暗号化コンテンツの復号処理を伴う再生処理となる。

【０１４７】

なお、コンテンツの購入処理を伴わない試聴処理においても、図２０を参照して説明した購入コンテンツの再生と同様、ＥＫＢ処理に基づくキー取得処理によってコンテンツ復号用のキーを取得することが必要となる。例えば、コンテンツ利用機器としてのハードウェアに対応して設定されたカテゴリツリーに対応するＥＫＢとしてのハード対応ＥＫＢ［ＥＫＢ（Ｈ）］と、コンテンツ利用サービスに対応して設定されたカテゴリツリーに対応するＥＫＢとしてのサービス対応ＥＫＢ［ＥＫＢ（Ｓ）］に対する正当なＤＮＫを有するユーザのみがコンテンツ再生を実行可能とする構成が適用でき、試聴においても再生権限を限定した範囲として設定可能となる。

【０１４８】

上述したように、クライアントは、ライセンスサーバに対する登録処理の際にデフォルト利用権情報（Ｄｅｆａｕｌｔ　Ｕｓａｇｅ　Ｒｉｇｈｔ）を取得し、コンテンツの購入処理を伴わない、試聴処理の際にデフォルト利用権情報に基づいてコンテンツ再生を可能とした構成であるので、ユーザは、コンテンツの購入を実行することなく、コンテンツの試聴再生が可能となり、また、試聴が許可されるクライアントは、ライセンスサーバに対する登録処理を行ない、デフォルト利用権情報を有するクライアントに限定されることになるので、試聴データが無秩序に氾濫してしまうことが防止される。

【０１４９】

なお、図２１のシーケンス図では、ストリーミング再生の例を示したが、試聴データをクライアントの記憶媒体に格納し、再生時に、デフォルト利用権情報（Ｄｅｆａｕｌｔ　Ｕｓａｇｅ　Ｒｉｇｈｔ）の有無を判定して、デフォルト利用権情報の記録に基づいて再生を行なう構成とすることも可能である。

【０１５０】

［７．バックアップ／リストア処理］

次にクライアントが購入したコンテンツまたはコンテンツ利用権情報についてのバックアップ処理、リストア処理について説明する。

【０１５１】

リストア処理は、クライアントのコンテンツ購入時、あるいは購入後の処理として実行されるコンテンツ対応のライセンス情報、すなわちサービスデータ、利用権情報の再取得、格納処理、あるいはコンテンツの再取得処理として実行される。

【０１５２】

処理態様としては、サービスデータ、利用権情報、コンテンツのいずれかの再取得、あるいはこれらの全データの再取得が可能である。以下に説明する実施例においては、サービスデータ、利用権情報、コンテンツ全データの再取得、格納処理シーケンス例を説明するが、必ずしもこれら全データを再取得する処理に限らず、いずれかのデータのみを選択的に再取得することも可能である。

【０１５３】

図２３以下を参照して、バックアップ／リストア処理の詳細について説明する。図２３は、クライアントアプリケーション、ブラウザを有するＰＣ等のクライアントと、ショップサーバ、コンテンツサーバ、ライセンスサーバ、および管理システムとの間で実行されるバックアップ／リストア処理における通信シーケンスの初期ステップを示している。以下、シーケンス図に示す処理について説明する。

【０１５４】

クライアントは、前述したコンテンツ購入処理に従って、正規にコンテンツ購入を行なったものとする。図２３に示すシーケンスは、コンテンツ購入に続いて実行されるシーケンスである。

【０１５５】

コンテンツ購入処理を実行したクライアントは、バックアップ／リストアデータの取得のためのデータファイルとしてのリストア処理要求ファイル［ｒｅｓｔｏｒｅ．ｄａｔ］を生成（ステップ（５０））する。リストア処理要求ファイル［ｒｅｓｔｏｒｅ．ｄａｔ］の構成を図２４に示す。

【０１５６】

図２４に示すように、リストア処理要求ファイル［ｒｅｓｔｏｒｅ．ｄａｔ］

は、ＥＫＢ配信ツリーにおけるクライアント識別データとしてのリーフＩＤと、ハッシュ（ｈａｓｈ）値、例えばＭＡＣ（Message Authentication Code）からなる検証データによって構成される。クライアントアプリケーションは、管理システムと共有する秘密の鍵を適用してリーフＩＤに基づく検証用データとしてのハッシュ値あるいはＭＡＣを算出し、リーフＩＤと検証用データからなるリストア処理要求ファイル［ｒｅｓｔｏｒｅ．ｄａｔ］を生成する。

【０１５７】

メッセージ認証符号（ＭＡＣ：Message authentication Code）は、データの改竄検証用のデータとして生成されるものである。ＤＥＳ暗号処理構成を用いたＭＡＣ値生成例を図２５に示す。図２５の構成に示すように対象となるメッセージを８バイト単位に分割し、（以下、分割されたメッセージをＭ１、Ｍ２、・・・、ＭＮとする）、まず、初期値（Initial Value（以下、ＩＶとする））とＭ１を排他的論理和する（その結果をＩ１とする）。次に、Ｉ１をＤＥＳ暗号化部に入れ、鍵（以下、Ｋ１とする）を用いて暗号化する（出力をＥ１とする）。続けて、Ｅ１およびＭ２を排他的論理和し、その出力Ｉ２をＤＥＳ暗号化部へ入れ、鍵Ｋ１を用いて暗号化する（出力Ｅ２）。以下、これを繰り返し、全てのメッセージに対して暗号化処理を施す。最後に出てきたＥＮがメッセージ認証符号（ＭＡＣ（Message Authentication Code））となる。

【０１５８】

ＭＡＣ値は、その生成元データが変更されると、異なる値になり、検証対象のデータ（メッセージ）に基づいて生成したＭＡＣと、記録されているＭＡＣとの比較を行い、一致していれば、検証対象のデータ（メッセージ）は変更、改竄がなされていないことが証明される。

【０１５９】

図２３のシーケンスに戻り説明を続ける。クライアントは、ブラウザを介して管理システムの提供するリストアページにアクセス（ステップ（５１））し、管理システムは、リストアページをクライアントのブラウザに提示（ステップ（５２））する。管理システムの提示するリストアページは、リストア処理要求ファイル［ｒｅｓｔｏｒｅ．ｄａｔ］のアップロード処理を実行する機能を持つペー

ジである。

【０１６０】

クライアントは、管理システムの提示するリストアページにおいて、クライアントアプリケーションの生成したリストア処理要求ファイル［ｒｅｓｔｏｒｅ．ｄａｔ］をアップロードする。リストア処理要求ファイル［ｒｅｓｔｏｒｅ．ｄａｔ］は、図２４を参照して説明したように、ＥＫＢ配信ツリーにおけるクライアント識別データとしてのリーフＩＤと、例えばＭＡＣ（Message Authentication Code）からなるハッシュ（ｈａｓｈ）値によって構成される。

【０１６１】

管理システムは、リストア処理要求ファイル［ｒｅｓｔｏｒｅ．ｄａｔ］を受信すると、クライアントと共有する秘密鍵を用いて、リーフＩＤに対するハッシュ値を算出し、算出ハッシュ値と、受信ハッシュ値の照合処理を行ない、受信データの検証（ステップ（５４））を行なう。算出ハッシュ値と、受信ハッシュ値が適合したことを条件として、バックアップ／リストア用の起動ファイルをクライアントに送信（ステップ（５５））する。起動ファイルの構成は、先に図１５を参照して説明したと同様のファイル構成を持つ。

【０１６２】

起動ファイルは、ブラウザからクライアントアプリケーションに渡され（ステップ（５６））、起動ファイルの記述、あるいは拡張子によって判別選択されるバックアップ／リストア実行プログラムを起動し、リストア処理を実行（ステップ（５７））する。

【０１６３】

バックアップ／リストア処理の処理対象としては、サービスデータ、コンテンツ、コンテンツ利用権情報がある。サービスデータは前述したようにライセンスサーバに対する登録処理によって取得可能であり、コンテンツはコンテンツサーバから取得可能である。また、利用権情報は、ライセンスサーバから取得される。バックアップ／リストア処理においても、これらの各データは、それぞれのサーバから取得することになる。

【０１６４】

まず、図２６を参照して、バックアップ／リストア用サービスデータの取得処理について説明する。基本的に、この処理は、先に説明したコンテンツ購入時のクライアント登録処理と同様の手続きに従ったものとなる。

【０１６５】

まず、クライアントアプリケーションは、登録要求をライセンスサーバに送信（ステップ（６１））する。この登録要求には、管理システムが生成した起動ファイル中に含まれるトランザクションＩＤ（ＴＩＤ）が含まれる。

【０１６６】

登録要求を受信したライセンスサーバは、トランザクションＩＤ（ＴＩＤ）に基づいて、バックアップ／リストア用サービスデータの取得であることを識別し、管理システムに対してサービス事前データ、すなわちサービスデータのバックアップ／リストア用データの割当要求（ステップ（６２））を行なう。管理システムは、同じトランザクションＩＤに基づいて処理を実行したクライアント端末があるか否かを管理データに基づいて検証し、ある場合には、これらを対応付けて記憶（ステップ（６３））する。これは、バックアップ／リストア処理の処理回数の上限（例えば３回）を設定し、上限を超える処理要求の場合には、処理を実行しないという設定を可能とするためである。

【０１６７】

管理データの更新処理を実行した管理システムは、サービス事前データ割当応答をライセンスサーバに送信（ステップ（６４））する。これは、バックアップ／リストア用サービスデータの発行許可情報として送信されるものである。

【０１６８】

サービス事前データ割当応答を受信したライセンスサーバは、バックアップ／リストア用サービスデータのクライアントに対する発行処理を実行（ステップ（６５））する。サービスデータは、先に図１７（ａ）を参照して説明したように、サービスデータ３７０には、ＥＫＢ配信ツリーにおいて設定されるクライアントに固有のリーフＩＤ、サービス識別子としてのサービスＩＤ、さらにデバイスノードキー（ＤＮＫ）をルートキー（Ｋｒｏｏｔ）で暗号化したデータ、Ｅ（Ｋｒｏｏｔ，ＤＮＫ）が含まれる。

【０１６９】

さらに、この処理時に、デフォルト利用権情報（図１７（ｂ）参照）もライセンスサーバからクライアントに対して発行される。先に説明したように、利用権情報は、通常は、購入コンテンツの利用条件を格納し、コンテンツの購入に対応して発行されるものであるが、デフォルト利用権情報は、コンテンツの購入を条件として発行するものではなく、クライアントの登録処理、あるいはサービスデータの発行処理を条件として発行する。このデフォルト利用権情報は、前述したようにコンテンツの試聴処理の際の有効な利用権情報として適用される。

【０１７０】

ライセンスサーバからサービスデータ、デフォルト利用権情報を受領したクライアントは、これらのデータをバックアップ用として、記憶手段に格納（ステップ（６６））する。

【０１７１】

次に、図２７を参照して、コンテンツのバックアップ／リストア処理について説明する。コンテンツのバックアップ／リストア処理実行の場合、クライアントアプリケーションは、コンテンツダウンロード要求をコンテンツサーバに対して実行（ステップ（７１））する。これは、先にクライアントが購入したコンテンツと同一である。クライアントアプリケーションは、コンテンツＩＤ（ＣＩＤ）によりコンテンツを指定してコンテンツダウンロード要求をコンテンツサーバに対して実行する。

【０１７２】

コンテンツサーバは、コンテンツダウンロード要求を受信すると、ＣＩＤに対応するコンテンツ情報をクライアントに送信（ステップ（７２））する。このコンテンツ情報は、暗号化コンテンツを含む情報である。先に図１７（ｃ）を参照して説明したように、コンテンツキー：Ｋｃで暗号化されたコンテンツデータ：Ｅｎｃ（Ｋｃ，Ｃｏｎｔｅｎｔ）、コンテンツキー：Ｋｃをルートキー：Ｋｒｏｏｔで暗号化したデータ：Ｅｎｃ（Ｋｒｏｏｔ，Ｋｃ）、さらに：ルートキー：Ｋｒｏｏｔを取得するためのＥＫＢ、さらに試聴フラグデータ、サービスＩＤ等の情報が付加されたファイルである。

【０１７３】

コンテンツ情報を受領したクライアントは、受信コンテンツに対応する利用権情報（Ｕｓａｇｅ　Ｒｉｇｈｔ）の取得要求をライセンスサーバに対して送信（ステップ（７３））する。この要求には、起動ファイル（図１５参照）中に含まれる利用権情報ＩＤ（ＵＩＤ）、クライアント識別データとしてのリーフＩＤ、トランザクションＩＤ（ＴＩＤ）が含まれる。

【０１７４】

ライセンスサーバは、利用権情報（Ｕｓａｇｅ　Ｒｉｇｈｔ）の取得要求を受信すると、管理システムに対して、注文照会処理（ステップ（７４））を行なう。この要求には、利用権情報ＩＤ（ＵＩＤ）、トランザクションＩＤ（ＴＩＤ）が含まれる。注文照会を受信した管理サーバは、注文照会応答として、利用権情報ＩＤ（ＵＩＤ）に対応する利用条件を設定した応答情報をライセンスサーバに送信（ステップ（７５））する。

【０１７５】

応答情報を受信したライセンスサーバは、コンテンツ利用条件を設定した利用権情報（Ｕｓａｇｅ　Ｒｉｇｈｔ）を生成して、クライアントに対して再発行（ステップ（７６））する。なお、コンテンツ利用条件とは、コンテンツの再生回数、期限、外部機器に対するコピー、チェツクアウト処理等の各種処理の許可情報によって構成される。

【０１７６】

利用権情報（Ｕｓａｇｅ　Ｒｉｇｈｔ）を受信したクライアントは、先に受信したコンテンツと利用権情報とを記憶手段にバックアップデータとして格納する。

【０１７７】

なお、バックアップ／リストア処理において、ライセンスサーバが発行する利用権情報は、正規なコンテンツ購入処理に際して発行する利用権情報とは異なる利用条件を設定したものとしてもよい。例えば、正規なコンテンツ購入時に発行する利用権情報に含まれる利用条件より厳しい条件、例えば利用期間の制限、コピー禁止、あるいはチェックアウト禁止といった条件を設定してバックアップ／

リストア処理用の利用権情報を設定発行してもよい。

【０１７８】

［８．リコメンドファイルによるコンテンツの二次配信］

次に、正規にコンテンツを購入したクライアントが、購入コンテンツを他のクライアントに提供するいわゆるコンテンツ二次配信を実行し、コンテンツ利用権をライセンスサーバから新たに配布することで、二次配信コンテンツを受領したクライアントにおいても正当なコンテンツ利用権を有することを条件としてコンテンツ利用を可能とし、さらに、コンテンツサーバからのコンテンツ配信負荷の軽減を実現した構成について説明する。

【０１７９】

前述したように、コンテンツを再生利用するクライアントは、コンテンツを利用するためには、コンテンツサーバから暗号化されたコンテンツを受け取るとともに、ライセンスサーバから、ライセンス情報、すなわちサービスデータと、コンテンツに対応する利用権情報を受領することが必要となる。

【０１８０】

ライセンス情報、すなわちサービスデータおよび利用権情報は、データ容量の小さいデータであるため、インターネット等の通信網を介した送受信が頻繁に行われたとしてもトラフィックの上昇も少なく、多大な配信時間がかかるといった問題は発生しない。しかし、一方、コンテンツは、音楽データ、画像データ、プログラム等様々であり、そのデータ容量も大きなものとなる。このような大容量のコンテンツを特定のコンテンツサーバから多くのクライアントに送信する場合には、送信時間が長くなり、コンテンツサーバの負担、ネットワークトラッフィックの上昇等、様々な問題を発生させる。また、通信中の通信エラーによるコンテンツ配信エラーのトラブルも発生しかねない。

【０１８１】

以下では、すでに正規なコンテンツを購入したクライアントの保有するコンテンツを他のクライアントに提供、すなわち二次配信を実行し、二次配信によるコンテンツの提供を受けたクライアントが、そのコンテンツのライセンス情報をライセンスサーバから受領することで、コンテンツサーバのクライアントに対する

コンテンツ送信の負荷を減少させたシステムについて説明する。

【０１８２】

図２８にコンテンツを正規に受領したクライアントが他のクライアントに提供するコンテンツファイルを生成する処理手順を説明したフローを示す。なお、他のクライアントに提供するコンテンツを含むデータファイルをリコメンドファイルと呼ぶ。リコメンドファイルには、暗号化されたコンテンツを含むコンテンツファイル、および必要に応じてそのコンテンツの説明ファイル（例えばＨＴＭＬファイル）が含まれる。

【０１８３】

図２８の処理フローについて説明する。図２８の処理を実行するクライアントは、前述したコンテンツ購入処理を実行し、正規にコンテンツを購入したクライアント、あるいは、リコメンドファイルを他のクライアントから受領し、その後の手続きにおいて正規なライセンスを取得したクライアントである。図２８の処理は、クライアントアプリケーション（図１のクライアントアプリケーション１２）の１つの実行プログラムとしてクライアントシステムとしての情報処理装置の制御手段（ＣＰＵ等）による制御の下に実行される。ステップＳ８０１において、クライアントは、自己のクライアント装置のディスプレイにリコメンドファイル作成画面を表示する。

【０１８４】

リコメンドファイル作成画面例を図２９に示す。クライアントが正規購入し、再生可能なコンテンツリスト６５１が中央に表示され、リコメンドファイルを生成する場合は、このコンテンツリスト６５１からコンテンツを選択（ステップＳ８０２）し、右側のリスト６５４にタイトル等を表示させる。コンテンツリスト６５１とリスト６５４間の移動処理は、移動スイッチ６５２、６５３の操作によって実行される。

【０１８５】

リコメンドファイル生成対象コンテンツが選択されると、ステップＳ８０３において、リコメンドファイル作成ボタン６５５が押下される。リコメンドファイル作成ボタン６５５が押下されると、ステップＳ８０４において、リコメンドフ

ファイル内にコンテンファイルに併せて説明ファイル、例えばＨＴＭＬによって記述された説明ファイルを生成格納するか否かを選択する。これはユーザが任意に選択可能である。

【０１８６】

リコメンドファイルには、図３０（ａ）に示すように、暗号化コンテンツを含むコンテンツファイル７２１とコンテンツ説明ファイル７２２とを組み合わせたリコメンドファイル７２０構成と、図３０（ｂ）に示すように、暗号化コンテンツを含むコンテンツファイル７２１のみからなるリコメンドファイル７３０構成との２つの態様があり、クライアントはその態様を自由に選択可能となる。

【０１８７】

ステップＳ８０４において、コンテンツ説明用ファイルの作成をしないと選択した場合は、図３０（ｂ）に示すコンテンツファイル７２１のみからなるリコメンドファイル７３０が生成される。

【０１８８】

コンテンツファイルの構成を図３１に示す。コンテンツファイル（ＭＱＴファイル）７２１には、暗号化コンテンツと、コンテンツ付加情報としてのメタ情報、さらにコンテンツ購入可能なショップを示すショップサーバＵＲＬ、コンテンツ識別子としてのコンテンツＩＤ（ＣＩＤ）が含まれる。

【０１８９】

なお、コンテンツファイルに格納される暗号化コンテンツは、コンテンツキーＫｃにより暗号化されたコンテンツであり、コンテンツキーＫｃは、有効化キーブロック（ＥＫＢ）配信ツリー構成を適用して提供される有効化キーブロック（ＥＫＢ）の復号により取得可能なキーの適用によってのみ取得可能なキーである。

【０１９０】

一方、ステップＳ８０４において、コンテンツ説明用ファイル作成を選択した場合は、ステップＳ８０６に進み、コンテンツ説明ファイル（ＨＴＭＬファイル）生成用の説明データ（メタデータ）をコンテンツ管理テーブルから取得する。コンテンツに対応するコンテンツ説明データは、上述したように暗号化コンテン

ツとともに、コンテンツファイル内にも格納されているが、正規にコンテンツ利用権を取得したクライアントは、コンテンツフィルから取り出したコンテンツ対応のメタデータをコンテンツ管理データとして、別ファイルに格納管理しており、リコメンドファイルにおいて生成される説明ファイル用のメタデータは、このコンテンツ管理データから抽出される。

【０１９１】

ステップＳ８０７において、コンテンツ管理データから抽出したメタデータを、クライアントアプリケーションに設定されたテンプレートＨＴＭＬファイルに貼り付ける処理を実行し、コンテンツ対応の説明用ＨＴＭＬファイルを生成し、ステップＳ８０８において、コンテンツファイルと説明用ＨＷＭＬファイルからなるリコメンドファイルを生成する。

【０１９２】

コンテンツ説明用データとしてのＨＴＭＬファイルの表示構成例を図３２に示す。図３２に示す例は、コンテンツが音楽データの場合の例である。説明用ファイルは、図３２に示すように、音楽コンテンツの楽曲タイトル、アーティスト、発売元等の情報リスト、さらに、各種の操作、処理に関する説明が記述されている。リコメンドファイルを他のクライアントから受理したクライアントは、まずこの説明ファイルをオープンすることになる。

【０１９３】

リコメンドファイルに格納されたコンテンツは暗号化されたコンテンツであり、正規なライセンス情報、すなわちサービスデータとコンテンツ対応の利用権情報を取得していない場合には再生することはできない。従って、リコメンドファイルを受領したクライアントがリコメンドファイルに格納されたコンテンツを利用する場合には、ライセンス情報を取得する手続きを実行することになる。

【０１９４】

このライセンス情報取得処理について、図３３、図３４の処理フローを参照して説明する。リコメンドファイルを受領したクライアントは、図３２に示す説明用ファイル（ＨＴＭＬファイル）をオープンし、試聴、購入コンテンツ配信サイトボタン７３１をクリック（ステップＳ８１１）する。このクリック処理により

、クライアントアプリケーションが起動（ステップＳ８１２）し、同じリコメンドファイルに格納されたコンテンツファイル（ＭＱＴファイル）（図３１参照）を読み出して、コンテンツファイルからコンテンツＩＤ（ＣＩＤ）とショップＵＲＬを抽出（ステップＳ８１３）する。

【０１９５】

このように、コンテンツ説明用ファイルの試聴、購入コンテンツ配信サイトボタン７３１は、コンテンツファイルからショップサーバＵＲＬを抽出し、抽出ＵＲＬをブラウザに出力する処理を実行するクライアントアプリケーションプログラムを起動するリンクデータとして構成されている。従って、リコメンドファイルを受領したクライアントが容易にショップに接続して購入手続きを実行することが可能となる。

【０１９６】

ステップＳ８１４において、コンテンツファイルから抽出したコンテンツＩＤ（ＣＩＤ）に基づいて、コンテンツファイル名を設定する。これはクライアントアプリケーションにおいて予め設定されたファイル名設定処理として実行され、例えばコンテンツのタイトル、アーティスト名、あるいはその複合データ等が適用される。ステップＳ８１５では、ステップＳ８１４５で設定したファイル名のコンテンファイルがクライアントの記憶部に格納される。

【０１９７】

次に、ステップＳ８１６において、ステップＳ８１３でコンテンツファイルから抽出したショップＵＲＬがブラウザに渡され、ブラウザは受領ＵＲＬに対応するショップページをショップサーバから読み出す。

【０１９８】

図３４の処理フローのステップＳ８３１において、ショップ画面がクライアントのディスプレイに表示される。以下の処理は、基本的には、前述したコンテンツの購入処理、試聴処理のいずれかの処理と同様であり、先に図１１、図１３、図１８、図２１に従って説明した処理に従うことになる。ただし、コンテンツ自体はすでにコンクライアントが、リコメンドファイルから取得済みであるので、コンテンツサーバカらのコンテンツ受領処理は、省略される。

【０１９９】

一連の処理の概略は、図３４の処理フローのステップＳ８３２以下に示す処理となる。まず、クライアントがショップサーバの提示するショップ画面において購入を指定してショップサーバに購入要求を出力すると、ショップサーバから購入用起動ファイルが送信される。これは、先に、図１５を参照して説明した起動ファイルと同様の構成を持つ。

【０２００】

次に、ステップＳ８３３において、起動ファイルからコンテンツ識別子としてのコンテンツＩＤ（ＣＩＤ）を取得する。次に、ステップＳ８３４において、コンテンツＩＤ（ＣＩＤ）に基づいて、コンテンツファイル名を算出する。クライアント装置にコンテンツを格納する際のコンテンツファイル名は、先の図３３のフローの説明で述べたようにコンテンツＩＤ（ＣＩＤ）に基づいて設定されることがクライアントアプリケーションにおいて規定され、ＣＩＤとファイル名の対応付けがなされている。

【０２０１】

ステップＳ８３５において、コンテンツＩＤ（ＣＩＤ）から算出したファイル名と同一のファイル名のファイルが自己のクライアント装置の記憶部に格納されているか否かを判定する。コンテンツが格納されていない場合は、ステップＳ８３７に進み、コンテンツサーバに接続して、コンテンツダウンロードを行なうことになる。この処理は、先に説明したコンテンツ購入時の処理と同様である。

【０２０２】

しかし、リコメンドファイルを受領しているクライアントは、先の図３３のフロー忠のステップＳ８１４，Ｓ８１５において、所定のファイル名を設定したコンテンツファイルを記憶部に格納しており、コンテンツのダウンロード処理は省略され、ステップＳ８３６のコンテンツ利用権情報の取得処理を実行し処理を終了することが可能となる。

【０２０３】

クライアントがコンテンツ再生を実行する際は、前述したように、コンテンツ利用権情報に格納されたコンテンツ識別子（ＣＩＤ）と再生対象コンテンツのコ

ンテンツ識別子（ＣＩＤ）との照合を行ないＣＩＤの一致を条件としてコンテンツ再生を実行する。また、有効化キーブロック（ＥＫＢ）配信ツリー構成を適用して提供される有効化キーブロック（ＥＫＢ）の復号によりコンテンツキーＫｃを取得し、取得したコンテンツキーＫｃを適用して暗号化コンテンツの復号処理を実行することにより、コンテンツを再生利用することが可能となる。

【０２０４】

このように、すでにコンテンツを保有しているクライアントが暗号化コンテンツを含むコンテンツファイルと、説明用ファイルからなるリコメンドファイルを他のクライアントに提供することで、他のクライアントがコンテンツ配信サーバへのアクセスなしにコンテンツを受領することが可能となる。他のクライアントは、利用権情報を取得することを条件としてコンテンツの利用が可能となる構成であるので、不正なコンテンツの利用は防止される。

【０２０５】

なお、図３４のフローにおいてはサービスデータの取得処理については省略してあるが、サービスデータを保有していないクライアントがリコメンドファイルを受領した場合には、ライセンスサーバに対するアクセスを実行して登録処理を行ない、サービスデータを取得することが必要となる。この登録処理手続きは、先に図１３、図１６を参照して説明した処理に対応する処理となる。

【０２０６】

以上、特定の実施例を参照しながら、本発明について詳解してきた。しかしながら、本発明の要旨を逸脱しない範囲で当業者が該実施例の修正や代用を成し得ることは自明である。すなわち、例示という形態で本発明を開示してきたのであり、限定的に解釈されるべきではない。本発明の要旨を判断するためには、冒頭に記載した特許請求の範囲の欄を参酌すべきである。

【０２０７】

なお、明細書中において説明した一連の処理はハードウェア、またはソフトウェア、あるいは両者の複合構成によって実行することが可能である。ソフトウェアによる処理を実行する場合は、処理シーケンスを記録したプログラムを、専用のハードウェアに組み込まれたコンピュータ内のメモリにインストールして実行

させるか、あるいは、各種処理が実行可能な汎用コンピュータにプログラムをインストールして実行させることが可能である。

【０２０８】

例えば、プログラムは記憶媒体としてのハードディスクやＲＯＭ（Read Only Memory)に予め記録しておくことができる。あるいは、プログラムはフレキシブルディスク、ＣＤ－ＲＯＭ(Compact Disc Read Only Memory)，ＭＯ(Magneto optical)ディスク，ＤＶＤ(Digital Versatile Disc)、磁気ディスク、半導体メモリなどのリムーバブル記録媒体に、一時的あるいは永続的に格納（記録）しておくことができる。このようなリムーバブル記録媒体は、いわゆるパッケージソフトウエアとして提供することができる。

【０２０９】

なお、プログラムは、上述したようなリムーバブル記録媒体からコンピュータにインストールする他、ダウンロードサイトから、コンピュータに無線転送したり、ＬＡＮ(Local Area Network)、インターネットといったネットワークを介して、コンピュータに有線で転送し、コンピュータでは、そのようにして転送されてくるプログラムを受信し、内蔵するハードディスク等の記憶媒体にインストールすることができる。

【０２１０】

なお、明細書に記載された各種の処理は、記載に従って時系列に実行されるのみならず、処理を実行する装置の処理能力あるいは必要に応じて並列的にあるいは個別に実行されてもよい。

【０２１１】

【発明の効果】

以上、説明したように、本発明の構成によれば、クライアントは、購入済みのコンテンツまたはライセンス情報としてのサービスデータ、または利用権情報を、正規なコンテンツ購入クライアントであることの確認を条件として、再取得可能となり、購入済みあるいは取得済みのデータの読み出しが不可能となった場合においてもバックアップされたデータに基づいて、コンテンツを利用することが可能となる。

【０２１２】

さらに、本発明の構成によれば、クライアントは、購入済みのコンテンツまたはライセンス情報としてのサービスデータ、または利用権情報の再取得処理に際し、リストア処理要求ファイルとして、有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つデータファイルを生成し、生成したリストア処理要求ファイルをクライアント識別データとして適用する構成としたので、正規なコンテンツ購入クライアントであることの確認が確実に実行される。

【図面の簡単な説明】

【図１】

本発明を適用したコンテンツ提供システムの概要を示す図である。

【図２】

クライアント、および各サーバ、管理システムの構成例を示す図である。

【図３】

各種キー、データの暗号化処理、配布処理について説明するツリー構成図である。

【図４】

各種キー、データの配布に使用される有効化キーブロック（ＥＫＢ）の例を示す図である。

【図５】

コンテンツキーの有効化キーブロック（ＥＫＢ）を使用した配布例と復号処理例を示す図である。

【図６】

有効化キーブロック（ＥＫＢ）のフォーマット例を示す図である。

【図７】

有効化キーブロック（ＥＫＢ）のタグの構成を説明する図である。

【図８】

ツリー構成におけるカテゴリ分割を説明する図である。

【図９】

ツリー構成におけるカテゴリ分割を説明する図である。

【図１０】

ツリー構成におけるカテゴリ分割の具体例を説明する図である。

【図１１】

コンテンツ購入、または試聴処理における各エンティテイ間の実行処理シーケンス（その１）を示す図である。

【図１２】

管理システムにおいて実行するトランザクションＩＤ生成、発行処理手順を示すフロー図である。

【図１３】

コンテンツ購入、または試聴処理における各エンティテイ間の実行処理シーケンス（その２）を示す図である。

【図１４】

管理システムにおいて実行するダウンロード許可処理手順を示すフロー図である。

【図１５】

起動ファイルのデータ構成例を示す図である。

【図１６】

クライアントにおいて実行する起動ファイルに基づくアプリケーション実行手順を示すフロー図である。

【図１７】

サービスデータ、利用権情報のデータ構成例を示す図である。

【図１８】

コンテンツ購入処理における各エンティテイ間の実行処理シーケンスを示す図である。

【図１９】

コンテンツ再生処理の概要を説明する図である。

【図２０】

有効化キーブロック（ＥＫＢ）を適用したコンテンツ復号、利用処理例を説明

する図である。

【図２１】

コンテンツ試聴処理における各エンティテイ間の実行処理シーケンスを示す図である。

【図２２】

試聴コンテンツ再生処理の概要を説明する図である。

【図２３】

ライセンスまたはコンテンツのバックアップ／リストア処理における各エンティテイ間の処理シーケンス（その１）を示す図である。

【図２４】

リストア処理要求ファイル［ｒｅｓｔｏｒｅ．ｄａｔ］の構成例を示す図である。

【図２５】

ＭＡＣ生成処理構成を示す図である。

【図２６】

ライセンスまたはコンテンツのバックアップ／リストア処理における各エンティテイ間の処理シーケンス（その２）を示す図である。

【図２７】

ライセンスまたはコンテンツのバックアップ／リストア処理における各エンティテイ間の処理シーケンス（その３）を示す図である。

【図２８】

リコメンドファイルの生成処理フローを示す図である。

【図２９】

リコメンドファイル生成画面を示す図である。

【図３０】

リコメンドファイル構成例を示す図である。

【図３１】

リコメンドファイル中に格納されるコンテンツファイルの構成例を示す図である。

【図３２】

リコメンドファイル中に格納されるコンテンツ説明ファイルの表示例を示す図である。

【図３３】

リコメンドファイルを受領したクライアントにおけるライセンス情報取得処理フロー（その１）を示す図である。

【図３４】

リコメンドファイルを受領したクライアントにおけるライセンス情報取得処理フロー（その２）を示す図である。

【符号の説明】

１０　クライアント
１１　ブラウザ
１２　クライアントアプリケーション
２１　ショップサーバ
２２　ライセンスサーバ
２３　コンテンツサーバ
３１　管理システム
１００　タイマ
１０１　ＣＰＵ(Central processing Unit)
１０２　ＲＯＭ (Read-Only-Memory)
１０３　ＲＡＭ (Random Access Memory)
１０４　暗号化復号部
１０５　コーデック部
１０６　入力部
１０７　出力部
１０８　記憶部
１０９　通信部
１１０　ドライブ
１１１　バス

１１２　入出力インタフェース

１２１　リムーバブル記録媒体

２０１　バージョン

２０２　デプス

２０３　データポインタ

２０４　タグポインタ

２０５　署名ポインタ

２０６　データ部

２０７　タグ部

２０８　署名

３０１　ルートキー

３０２　ノードキー

３０３　リーフキー

３０４　カテゴリノード

３５０　ルートノード

３５１　Ｔシステムノード

３５２　Ｔサービスノード

３５３　Ｔハードノード

３５４　サービスプロバイダノード

３５５　リーフ

３６０　起動ファイル

３７０　サービスデータ

３７１　利用権情報

３７２　コンテンツ

３７３　試聴フラグ

３８１　ライセンスサーバ

３８２　コンテンツサーバ

３８３　クライアント

３８４　コンテンツ

４０１　サービスデータ

４０２　暗号化コンテンツファイル

４０３　利用権情報

４１１　ＥＫＢ（Ｈ）

６０１　リストア処理要求ファイル

６５１　コンテンツリスト

６５２，６５３　スイッチ

６５３　リコメンドファイル作成ボタン

６５４　リスト

７２０，７３０　リコメンドファイル

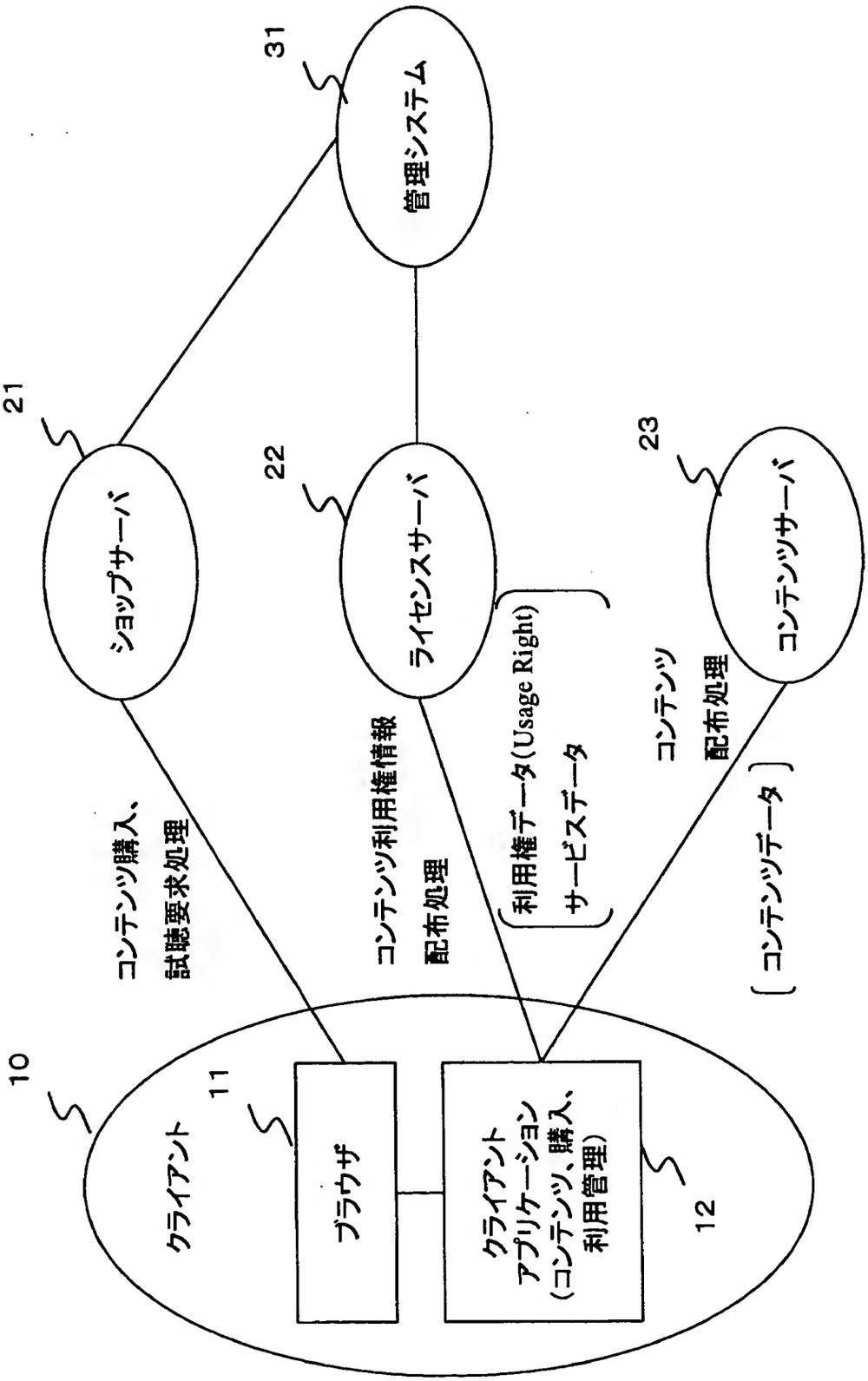
７２１　コンテンツファイル

７２２　コンテンツ説明ファイル

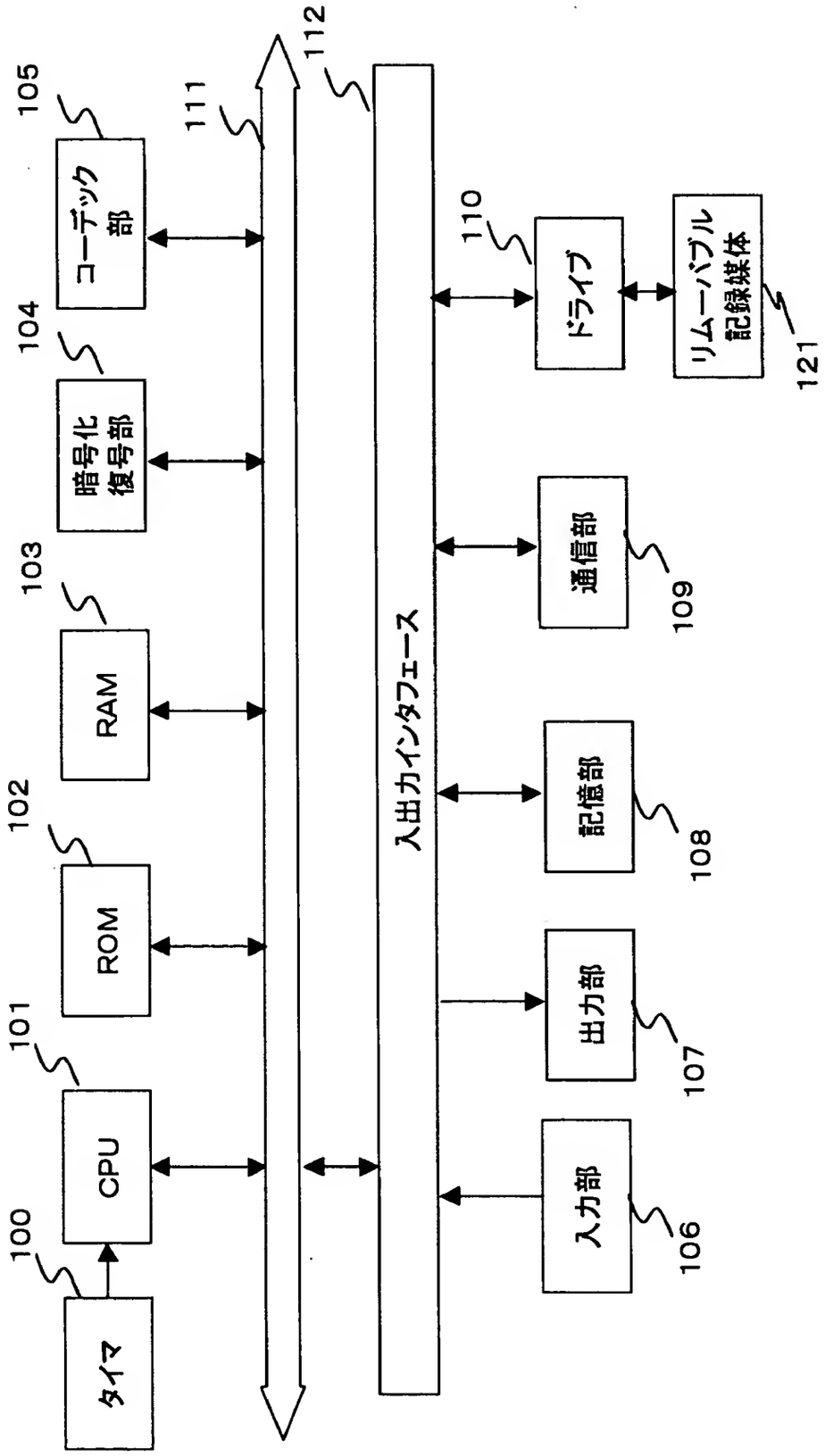
７３１　試聴、購入コンテンツ配信サイトボタン

【書類名】　　図面

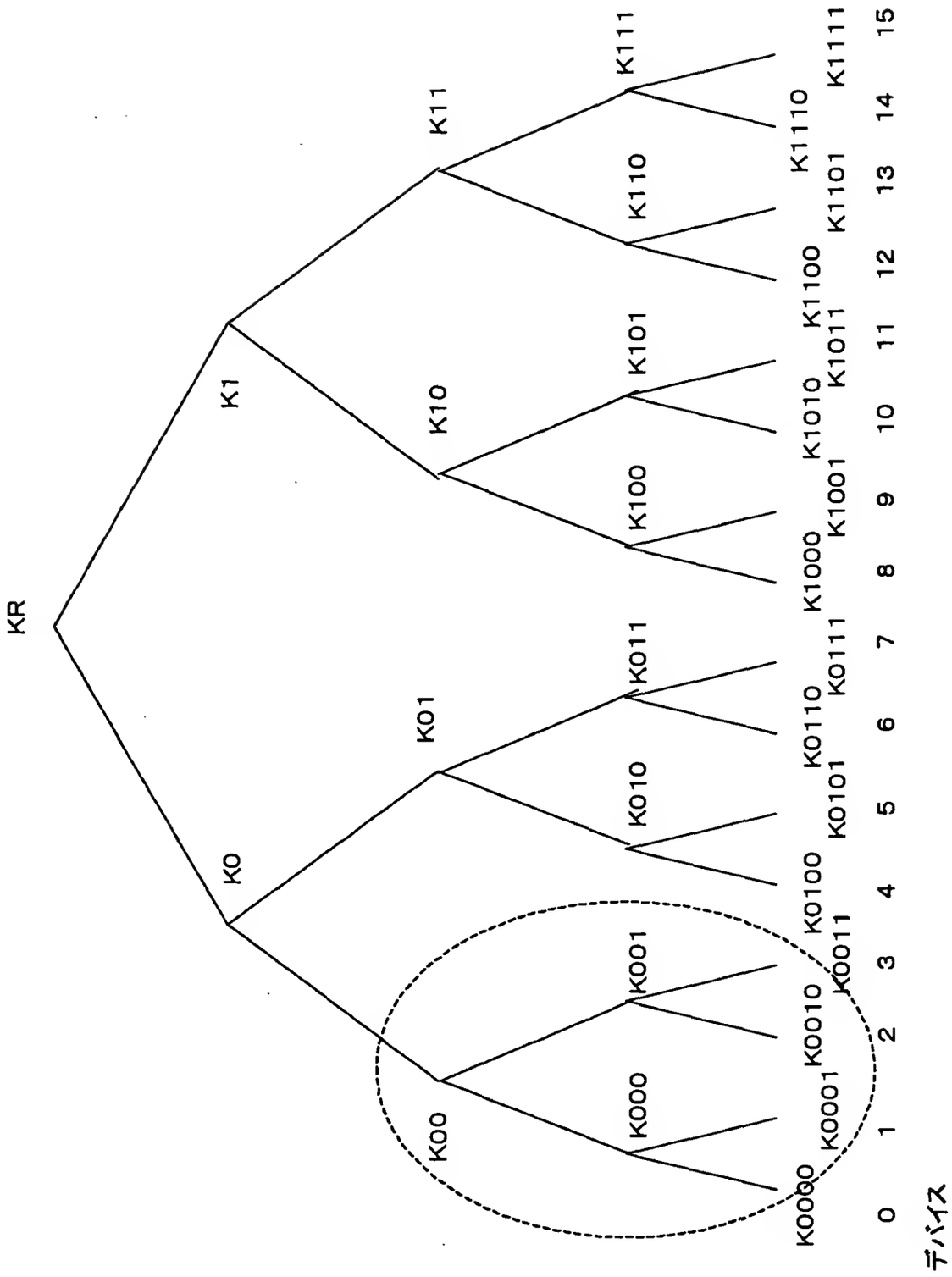
【図１】


31
管理システム
21
ショップサーバ
22
ライセンスサーバ
23
コンテンツサーバ
コンテンツ購入、
試聴要求処理
コンテンツ利用権情報
配布処理
利用権データ(Usage Right)
サービスデータ
コンテンツ
配布処理
コンテンツデータ
10
クライアント
11
ブラウザ
クライアント
アプリケーション
(コンテンツ、購入、
利用管理)
12

【図２】


タイマ
CPU
ROM
RAM
暗号化復号部
コーデック部
入出力インタフェース
ドライブ
通信部
記憶部
出力部
入力部
リムーバブル記録媒体
100
101
102
103
104
105
106
107
108
109
110
111
112
121

【図３】


KR
K0
K1
K00
K01
K10
K11
K000
K001
K010
K011
K100
K101
K110
K111
K0000
K0001
K0010
K0011
K0100
K0101
K0110
K0111
K1000
K1001
K1010
K1011
K1100
K1101
K1110
K1111
0
1
2
3
4
5
6
7
8
9
10
11
12
13
14
15
デバイス

【図４】

(A) 有効化キーブロック

(EKB:Enabling Key Block)例1

デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
0	Enc(K(t)0, K(t)R)
00	Enc(K(t)00, K(t)0)
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

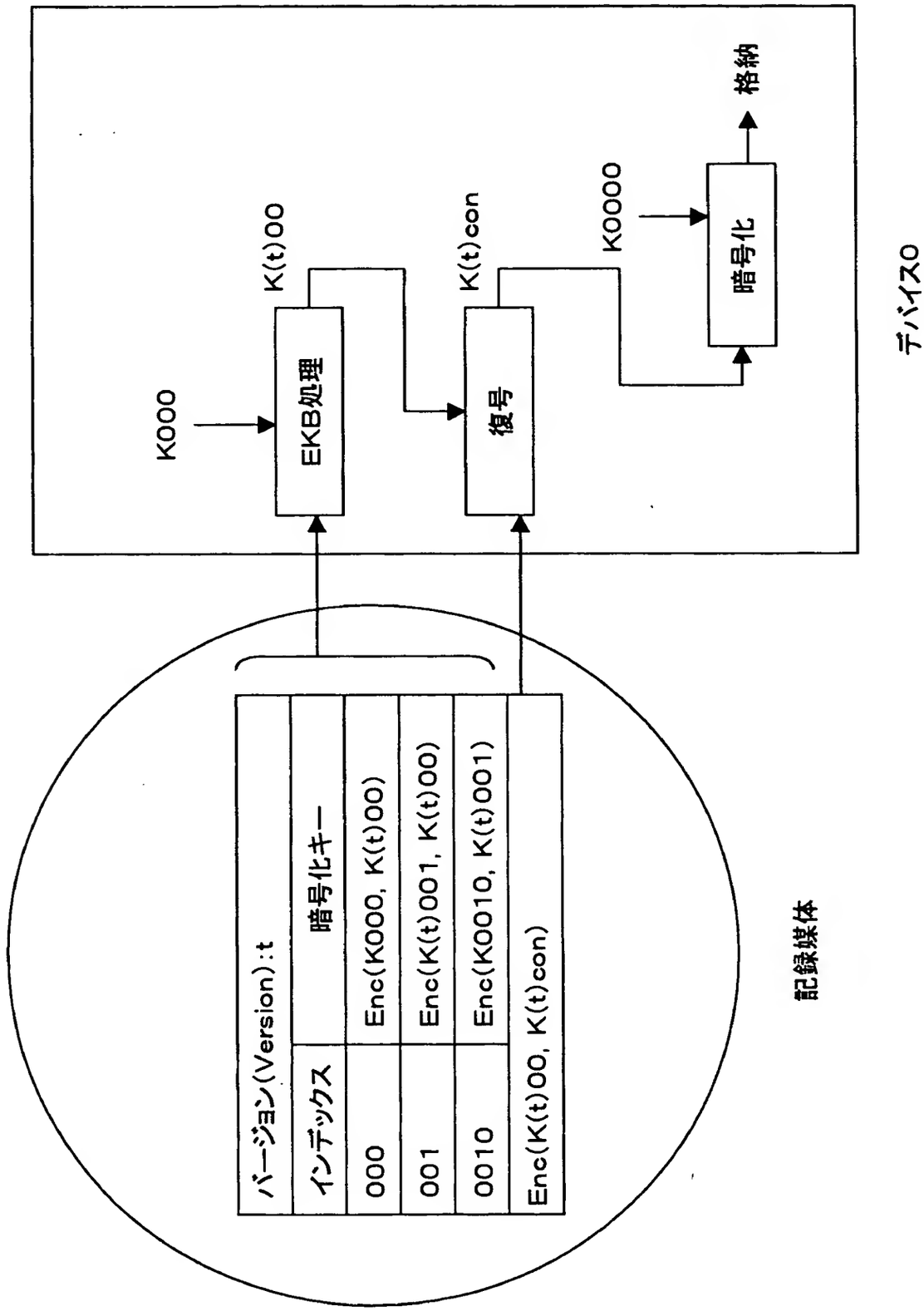
(B) 有効化キーブロック

(EKB:Enabling Key Block) 例2

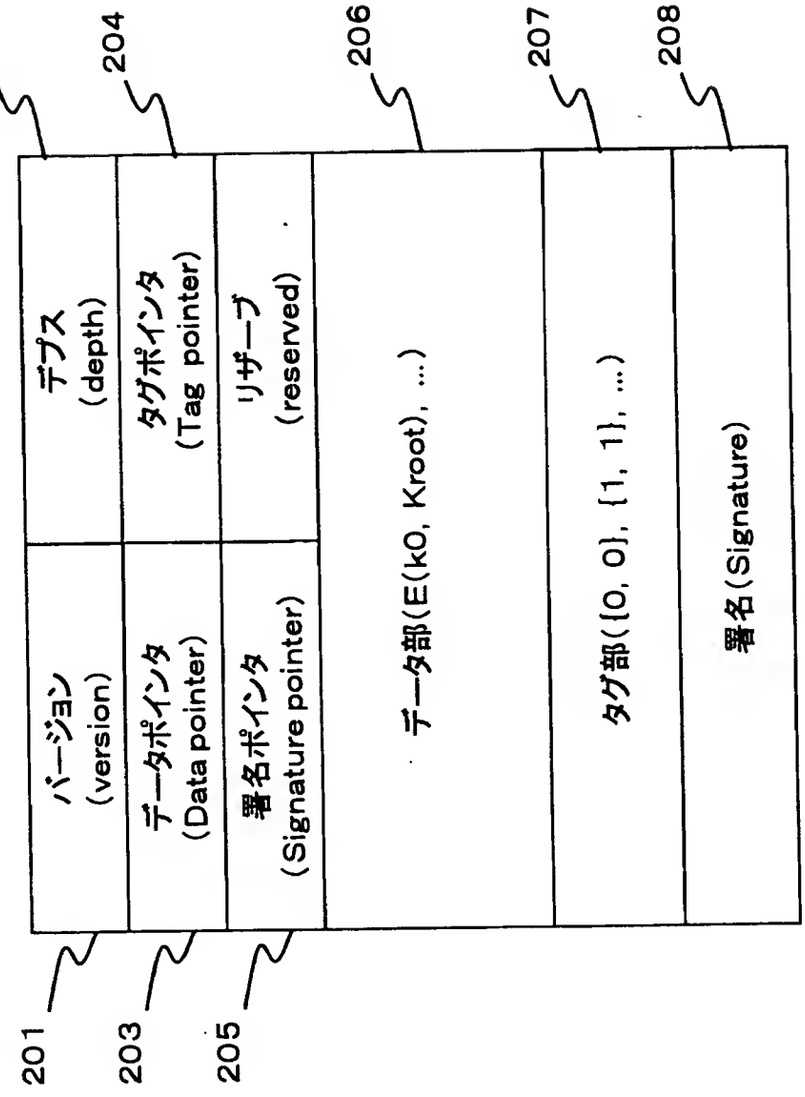
デバイス0, 1, 2にバージョン:tのノードキーを送付

バージョン(Version):t	
インデックス	暗号化キー
000	Enc(K000, K(t)00)
001	Enc(K(t)001, K(t)00)
0010	Enc(K0010, K(t)001)

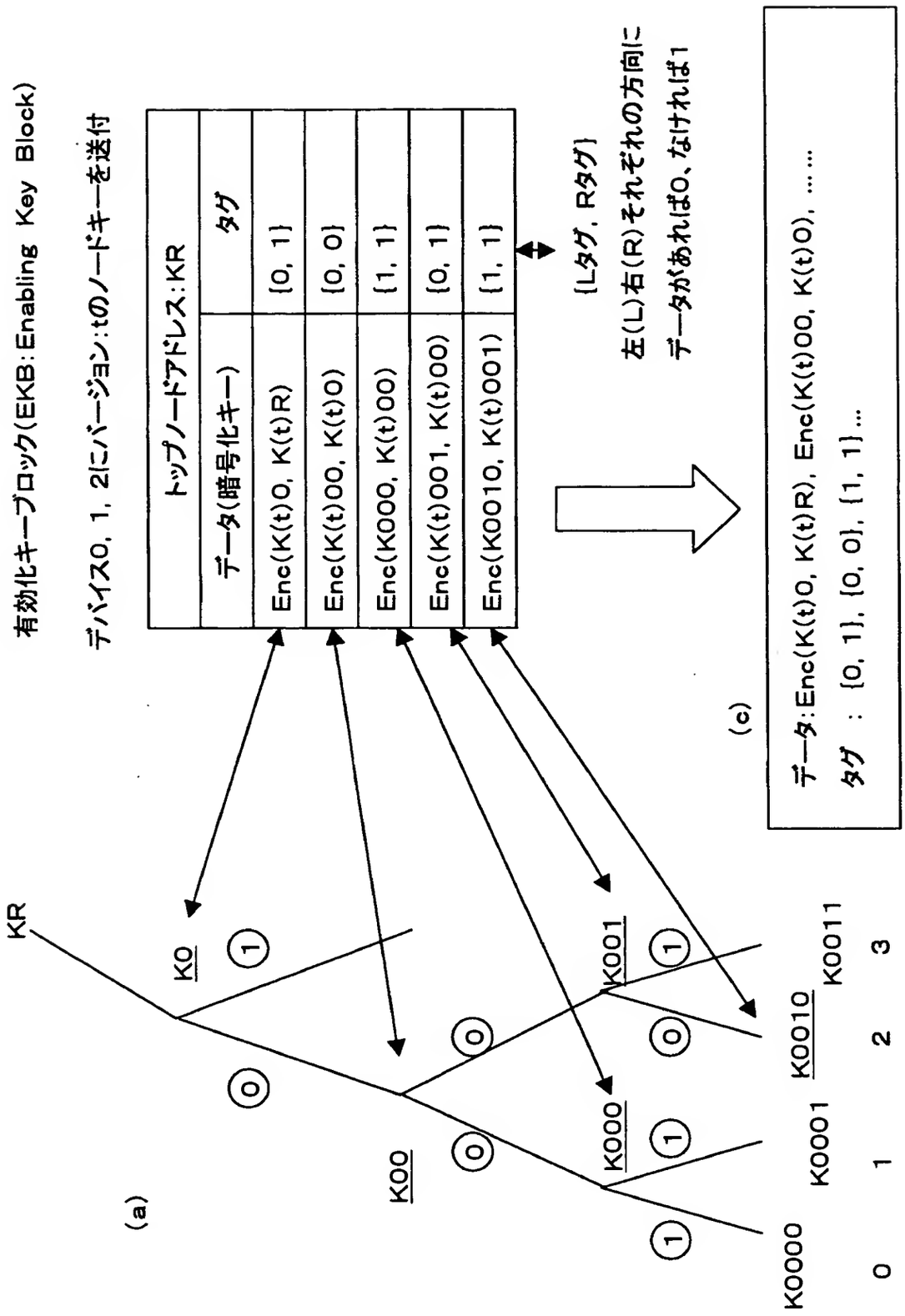
【図５】


K000
EKB処理
K(t)00
復号
K(t)con
K0000
暗号化
格納
デバイス0
記録媒体
バージョン(Version):t
インデックス
暗号化キー
000
Enc(K000, K(t)00)
001
Enc(K(t)001, K(t)00)
0010
Enc(K0010, K(t)001)
Enc(K(t)00, K(t)con)

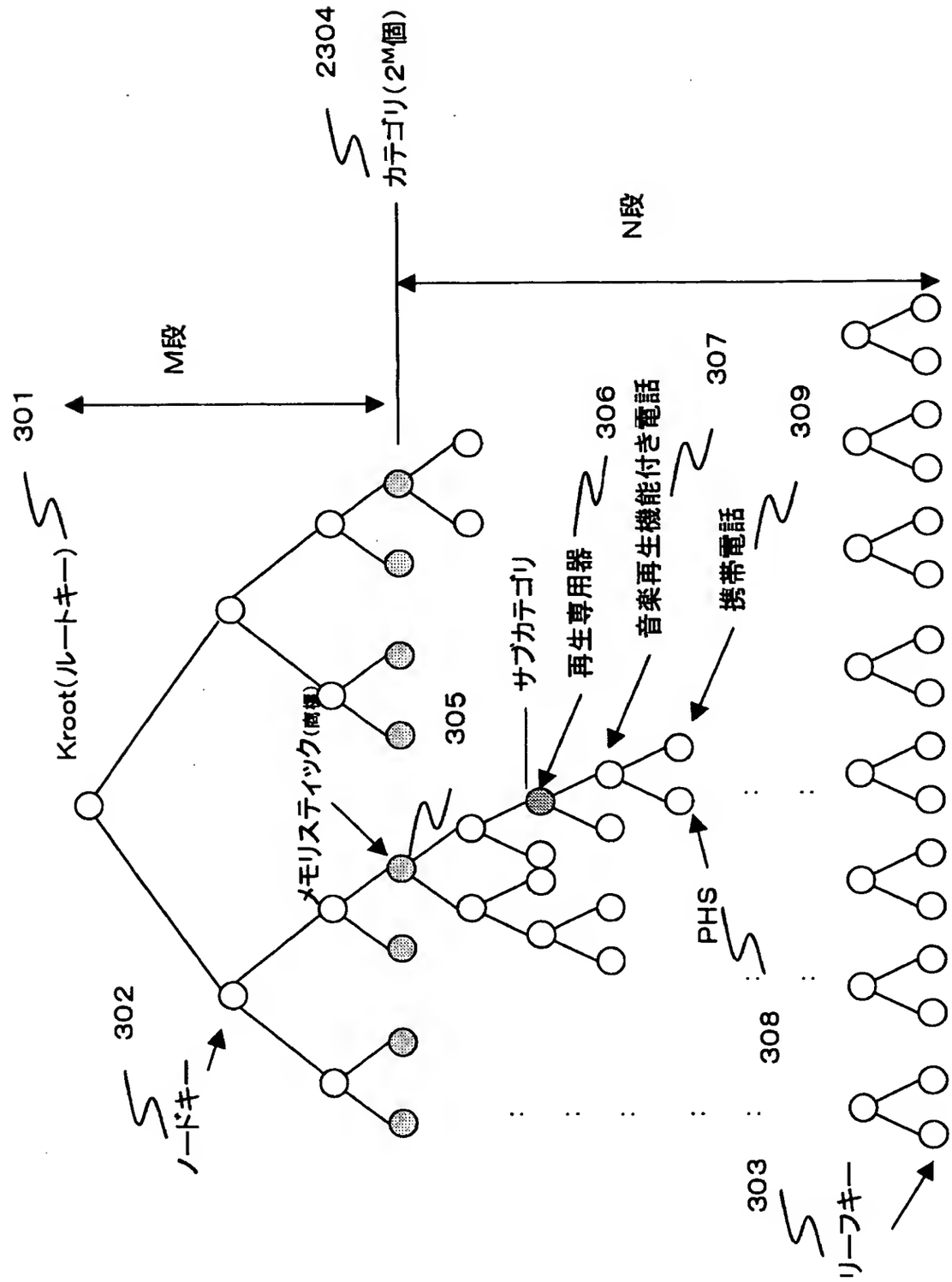
【図６】


202
204
206
207
208
デプス (depth)
タグポインタ (Tag pointer)
リザーブ (reserved)
バージョン (version)
データポインタ (Data pointer)
署名ポインタ (Signature pointer)
データ部(E(kO, Kroot), ...)
タグ部({O, O}, {1, 1}, ...)
署名(Signature)
201
203
205

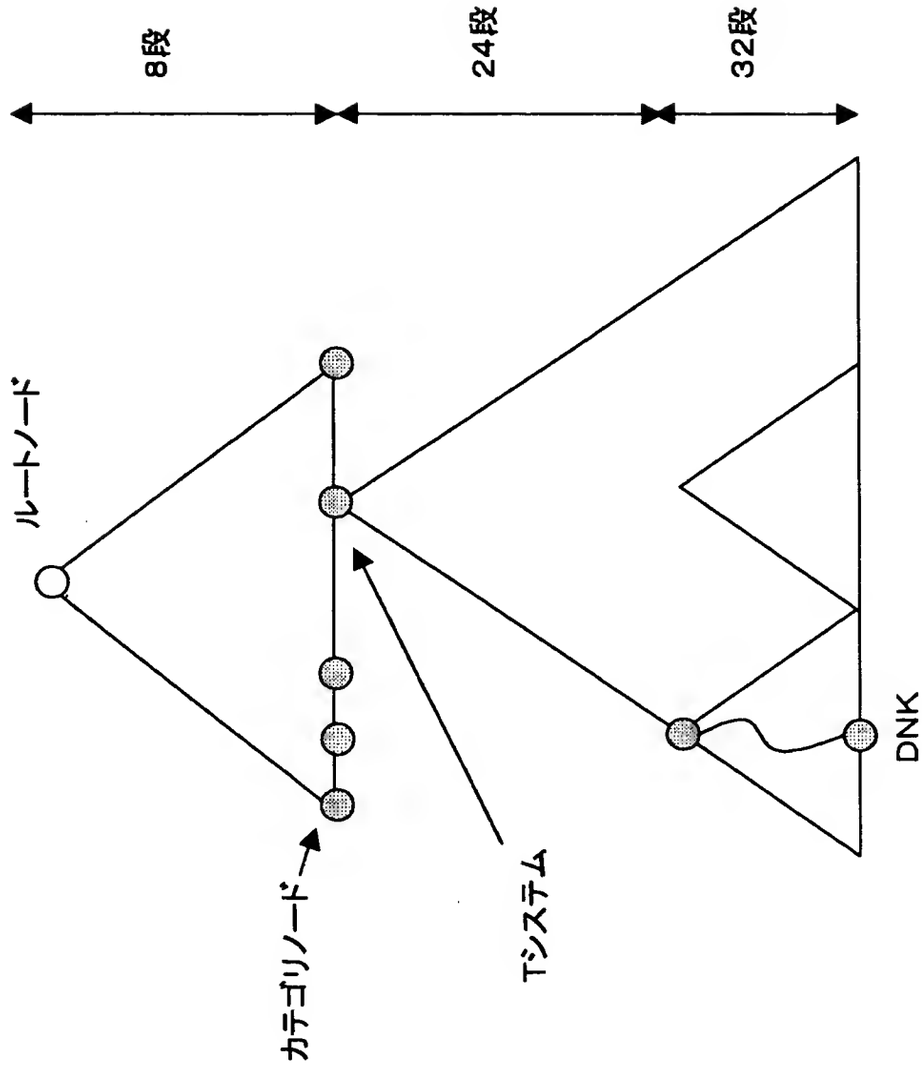
【図７】


(a)
KR
K0
K00
K000
K0000
K0001
K0010
K0011
K001
0
1
2
3
(b)
有効化キーブロック(EKB:Enabling Key Block)
デバイス0, 1, 2にバージョン:tのノードキーを送付
トップノードアドレス:KR
データ(暗号化キー)
タグ
Enc(K(t)0, K(t)R)
{0, 1}
Enc(K(t)00, K(t)0)
{0, 0}
Enc(K000, K(t)00)
{1, 1}
Enc(K(t)001, K(t)00)
{0, 1}
Enc(K0010, K(t)001)
{1, 1}
{Lタグ, Rタグ}
左(L)右(R)それぞれの方向に
データがあれば0、なければ1
(c)
データ:Enc(K(t)0, K(t)R), Enc(K(t)00, K(t)0), ……
タグ : {0, 1}, {0, 0}, {1, 1}…

【図８】

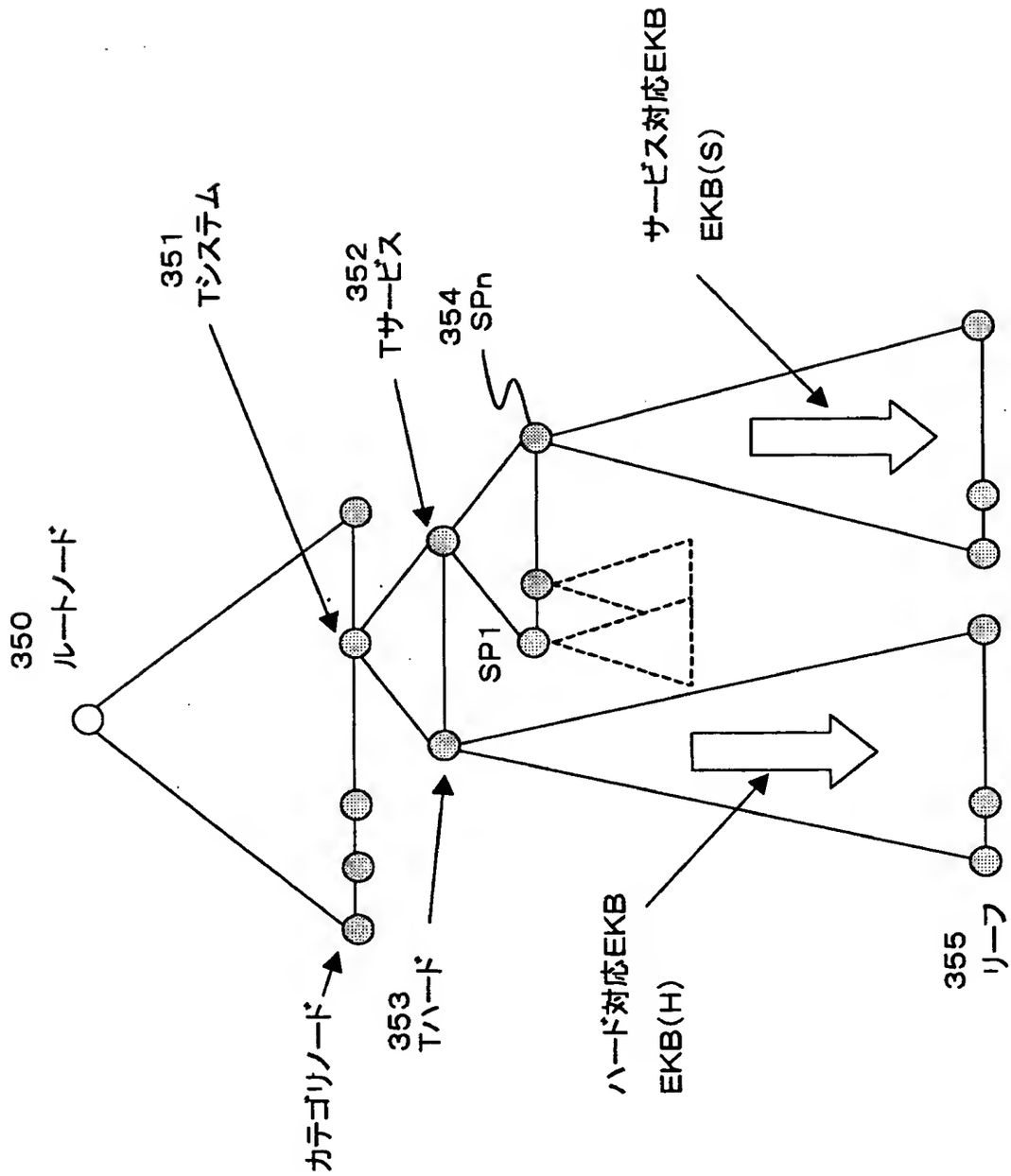

2304
カテゴリ(2M個)
N段
M段
301
Kroot(ルートキー)
306
再生専用器
307
音楽再生機能付き電話
309
携帯電話
サブカテゴリ
305
メモリスティック(商標)
PHS
302
ノードキー
308
303
リーフキー

【図９】

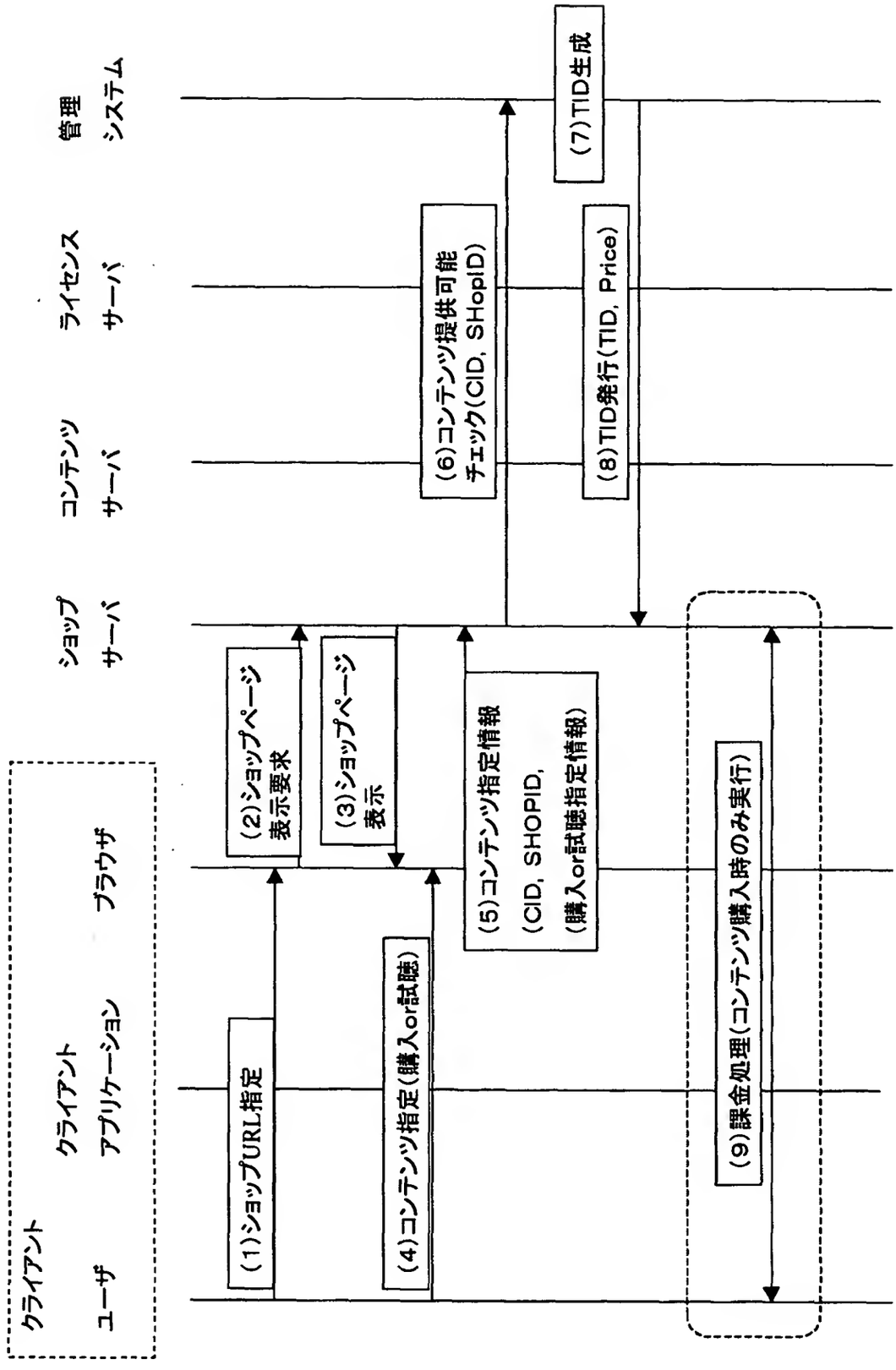


出証特２００３－３０４２４５９

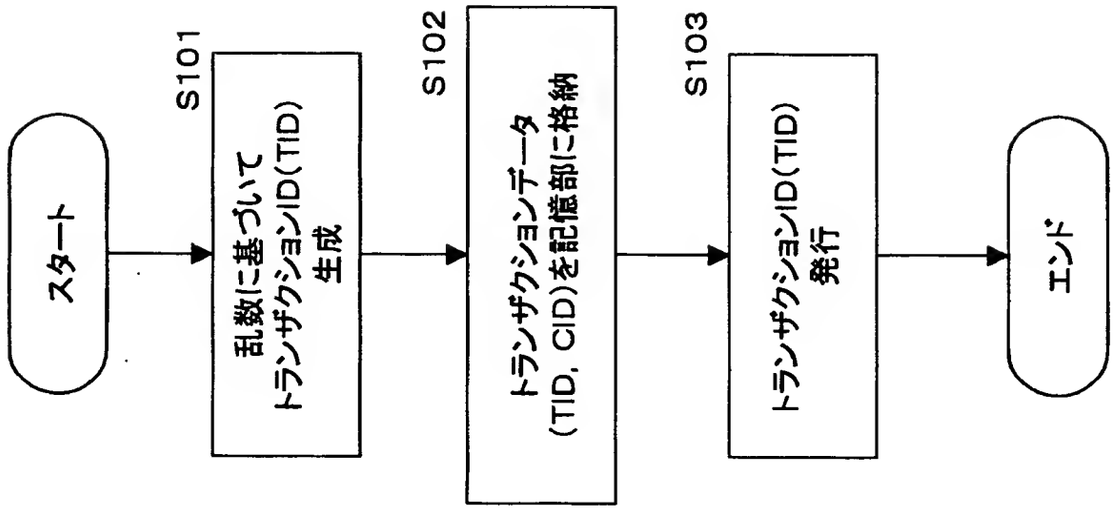
【図１０】


350
ルートノード
351
Tシステム
352
Tサービス
354
SPn
SP1
サービス対応EKB
EKB(S)
カテゴリノード
353
Tハード
ハード対応EKB
EKB(H)
355
リーフ

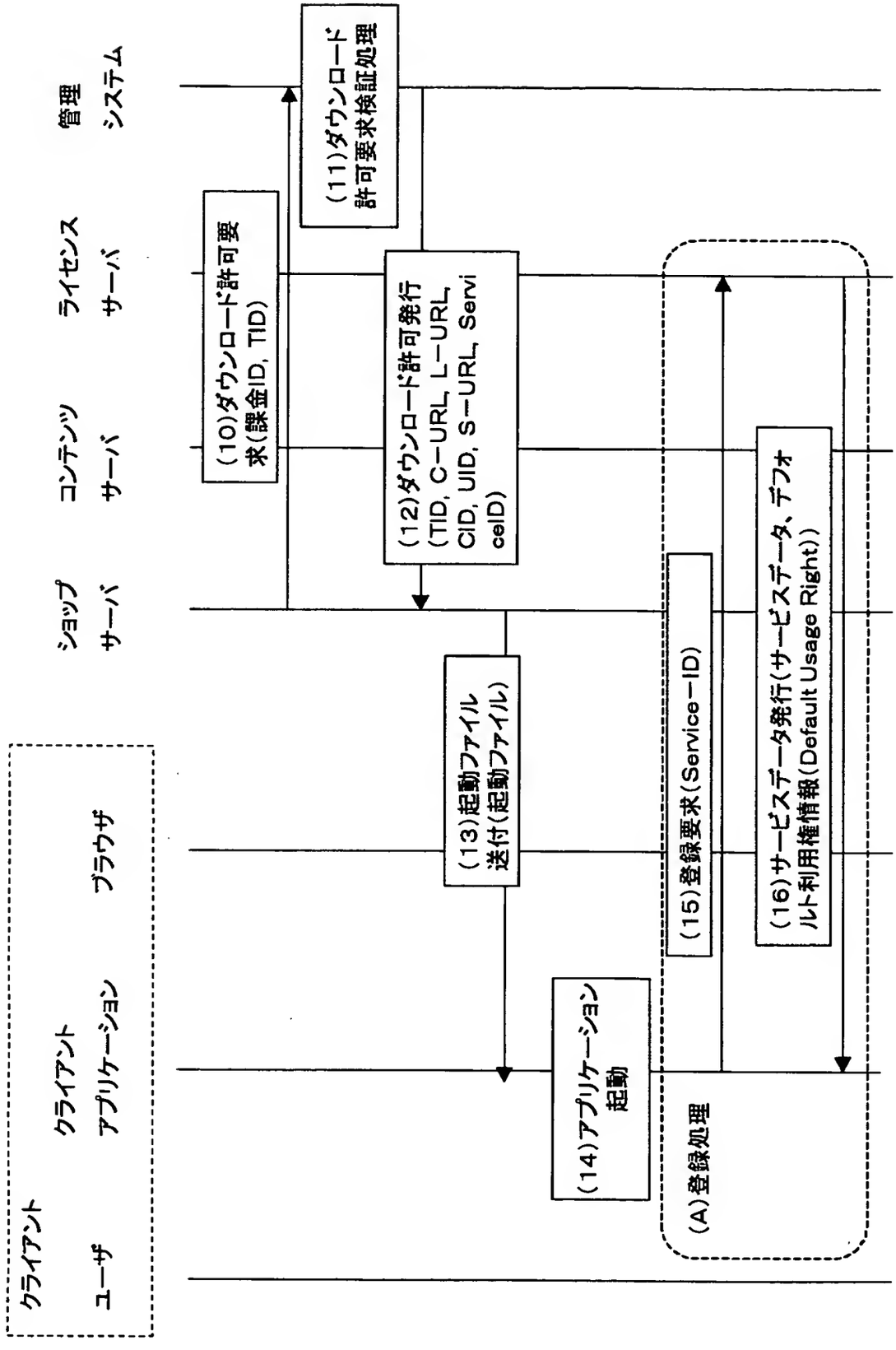
【図１１】


クライアント
ユーザ
クライアント
アプリケーション
ブラウザ
ショップ
サーバ
コンテンツ
サーバ
ライセンス
サーバ
管理
システム
(1)ショップURL指定
(2)ショップページ
表示要求
(3)ショップページ
表示
(4)コンテンツ指定(購入or試聴)
(5)コンテンツ指定情報
(CID, SHOPID,
(購入or試聴指定情報)
(6)コンテンツ提供可能
チェック(CID, SHopID)
(7)TID生成
(8)TID発行(TID, Price)
(9)課金処理(コンテンツ購入時のみ実行)

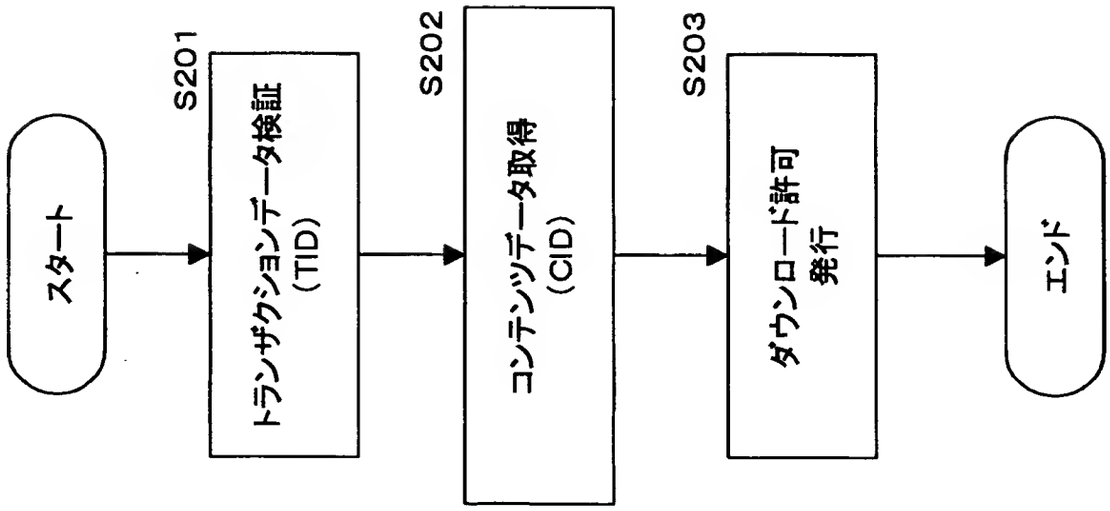
【図１２】


スタート
S101
乱数に基づいて
トランザクションID(TID)
生成
S102
トランザクションデータ
(TID, CID)を記憶部に格納
S103
トランザクションID(TID)
発行
エンド

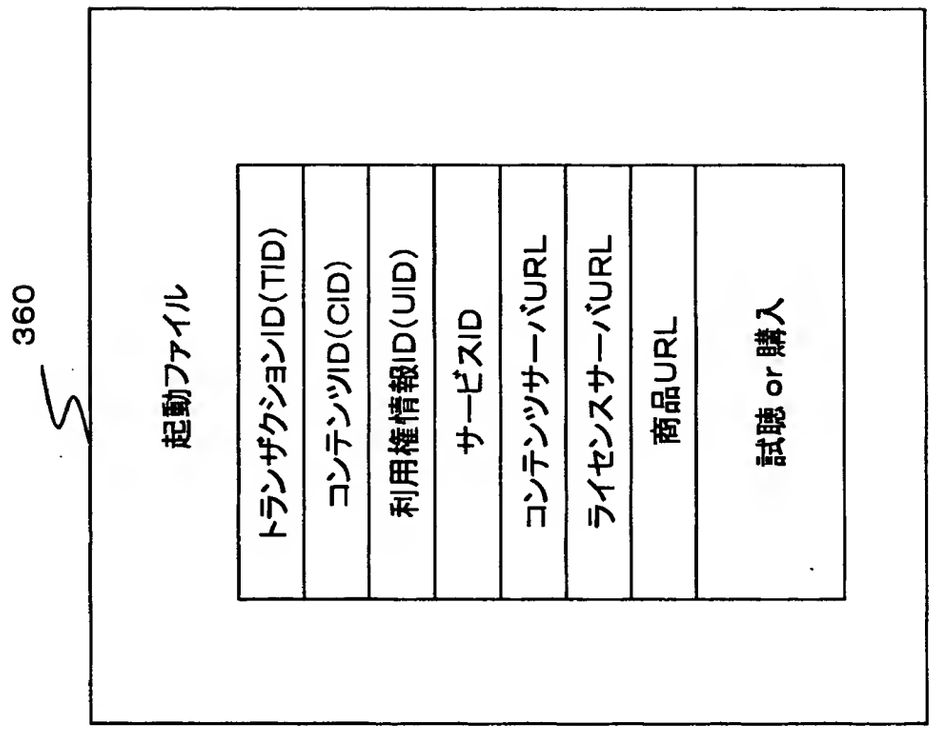
【図１３】


クライアント
ユーザ
クライアント
アプリケーション
ブラウザ
ショップ
サーバ
コンテンツ
サーバ
ライセンス
サーバ
管理
システム
(10)ダウンロード許可要求(課金ID, TID)
(11)ダウンロード許可要求検証処理
(12)ダウンロード許可発行(TID, C－URL, L－URL, CID, UID, S－URL, ServiceID)
(13)起動ファイル送付(起動ファイル)
(14)アプリケーション起動
(15)登録要求(Service－ID)
(16)サービスデータ発行(サービスデータ、デフォルト利用権情報(Default Usage Right))
(A)登録処理

【図１４】

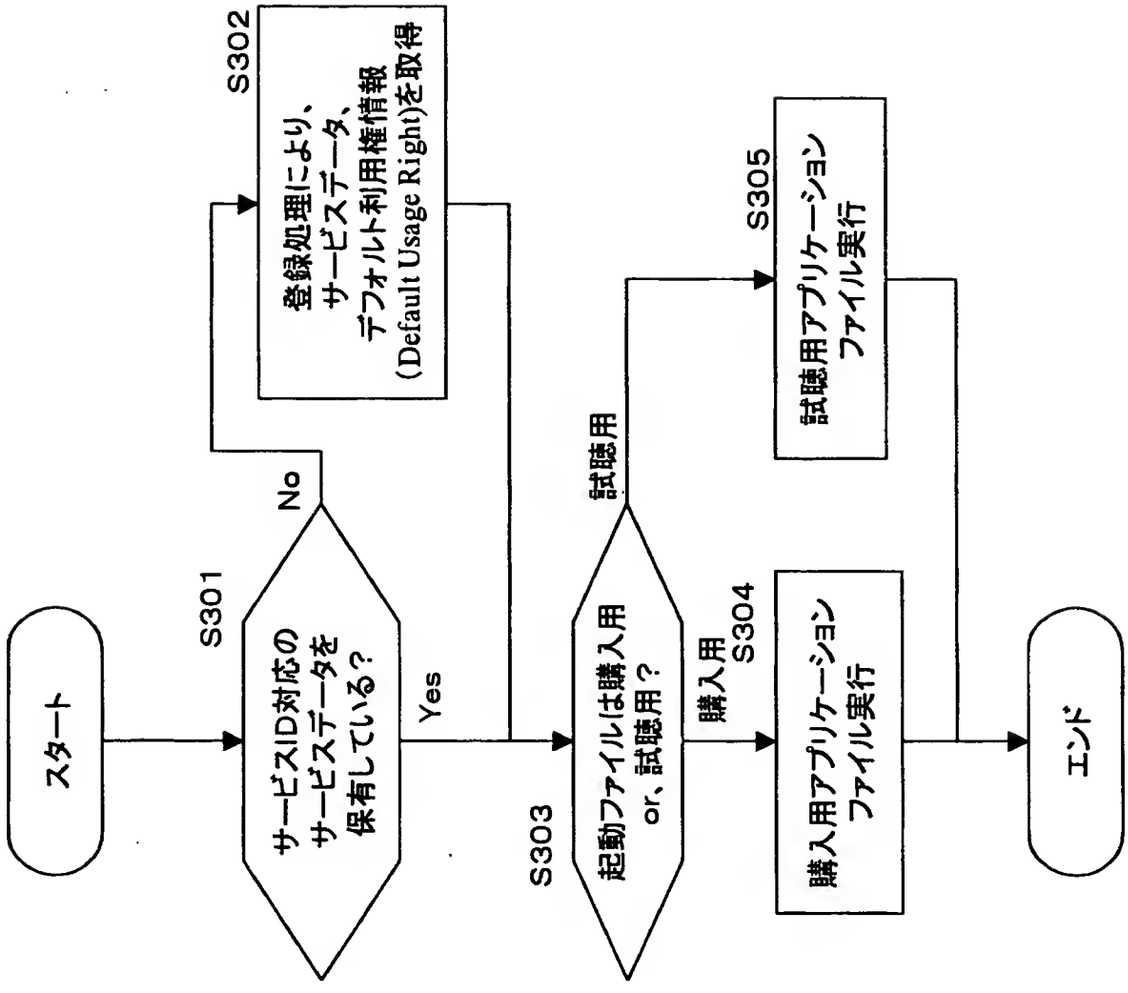

スタート
S201
トランザクションデータ検証
(TID)
S202
コンテンツデータ取得
(CID)
S203
ダウンロード許可
発行
エンド

【図１５】

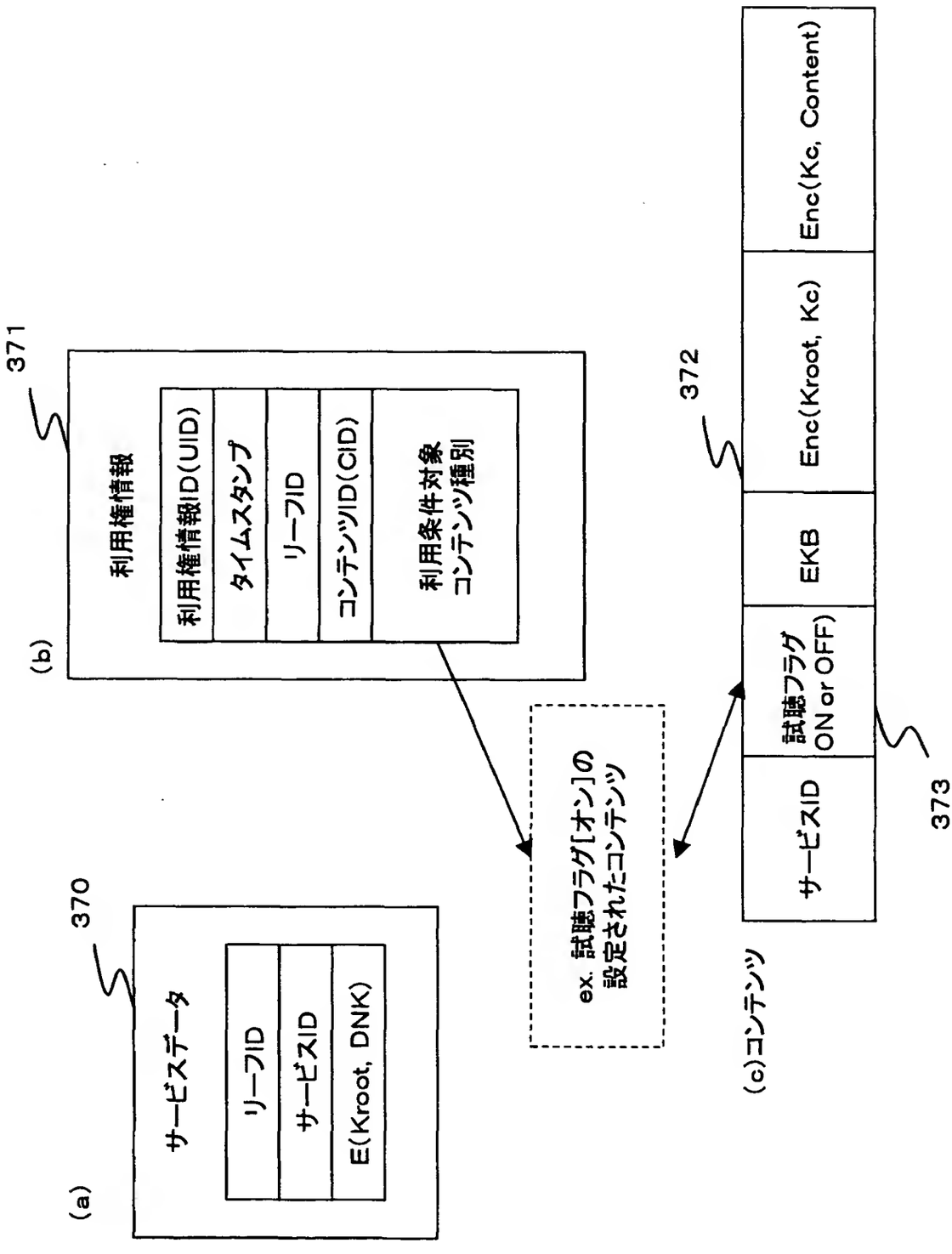


出証特２００３－３０４２４５９

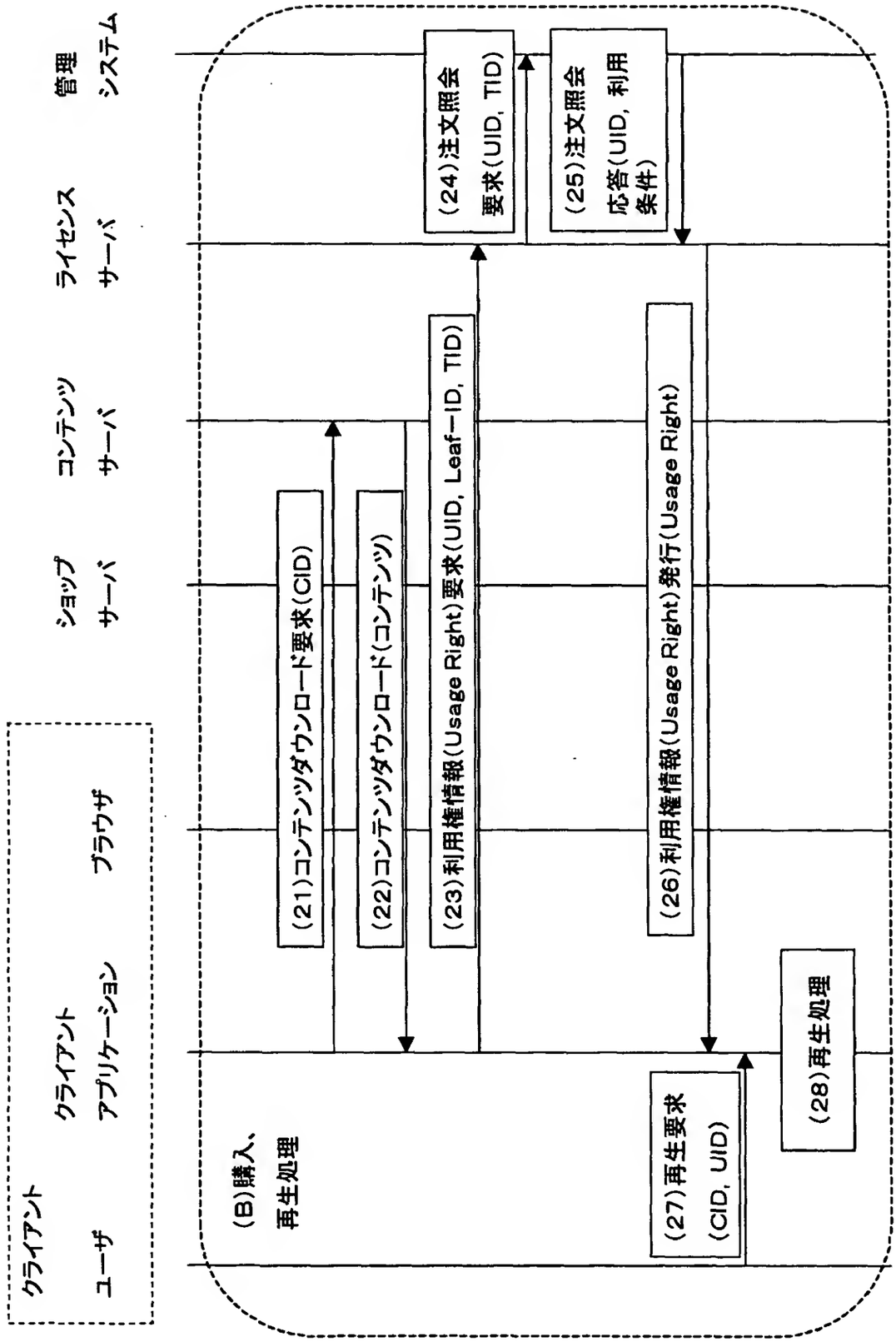
【図１６】


スタート
S301
サービスID対応の
サービスデータを
保有している？
No
Yes
S302
登録処理により、
サービスデータ、
デフォルト利用権情報
(Default Usage Right)を取得
S303
起動ファイルは購入用
or、試聴用？
試聴用
購入用
S304
購入用アプリケーション
ファイル実行
S305
試聴用アプリケーション
ファイル実行
エンド

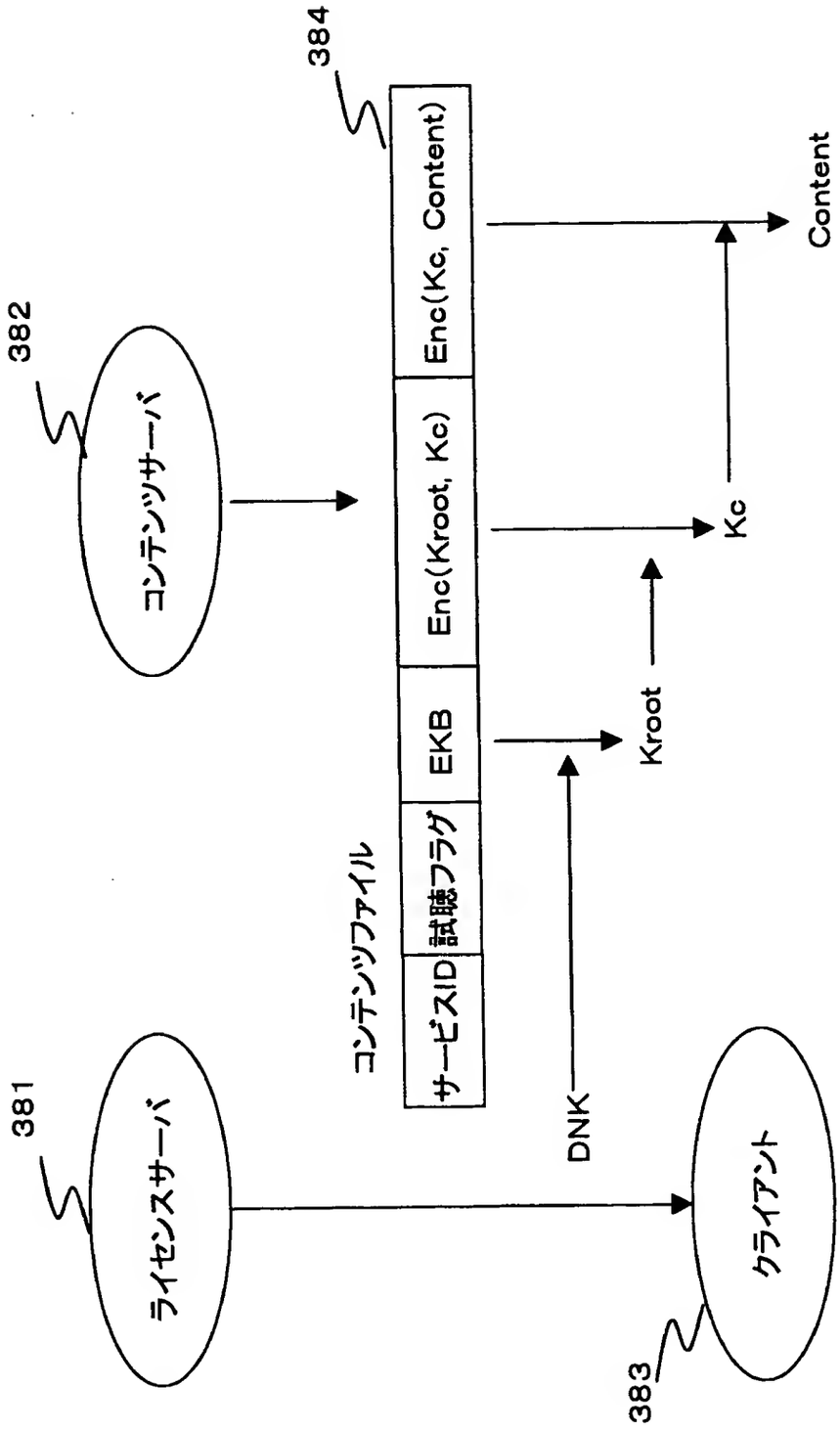
【図１７】


(a)
370
サービスデータ
リーフID
サービスID
E(Kroot, DNK)
(b)
371
利用権情報
利用権情報ID(UID)
タイムスタンプ
リーフID
コンテンツID(CID)
利用条件対象
コンテンツ種別
ex. 試聴フラグ[オン]の
設定されたコンテンツ
(c)コンテンツ
372
Enc(Kc, Content)
Enc(Kroot, Kc)
EKB
試聴フラグ
ON or OFF)
サービスID
373

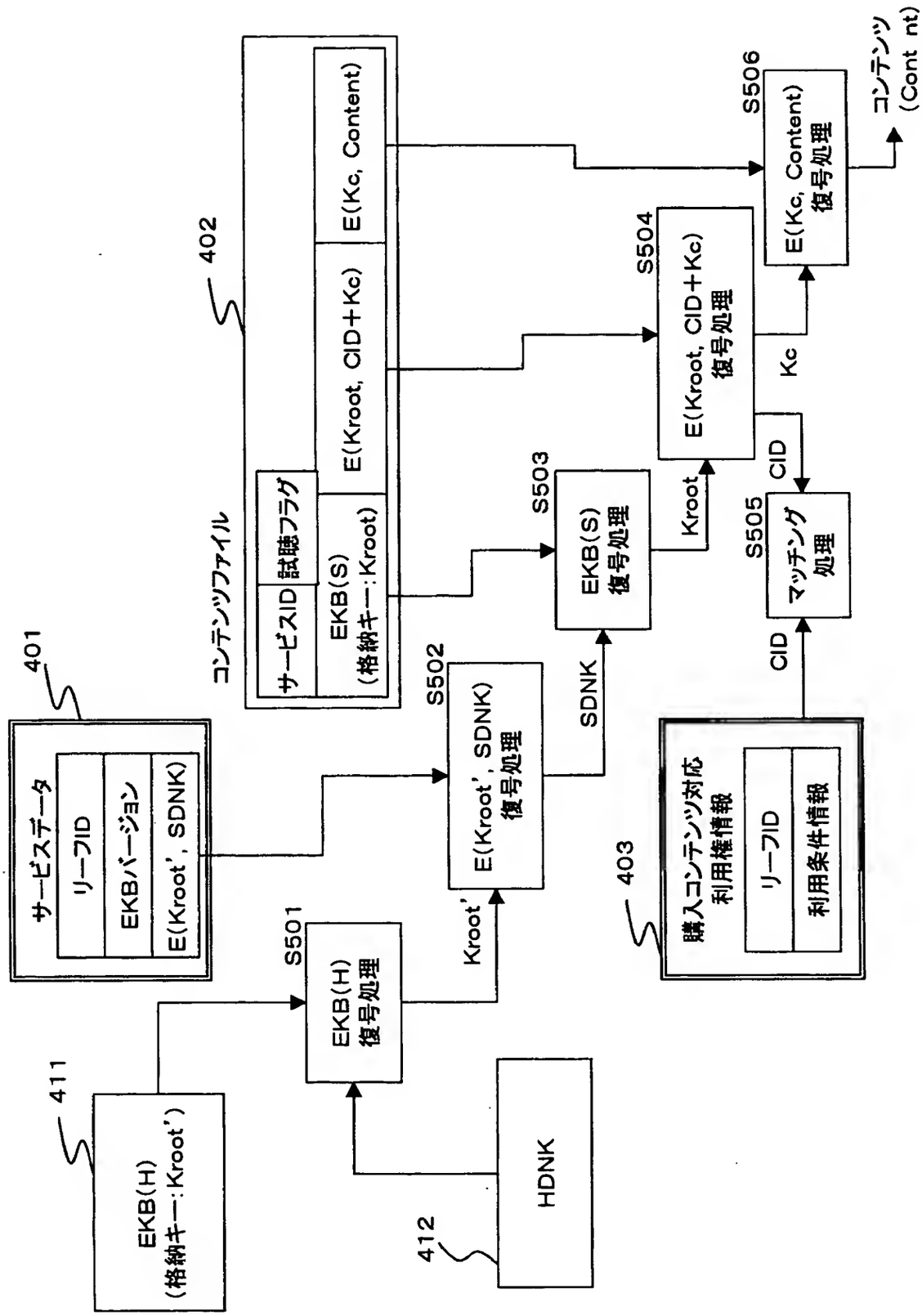
【図１８】


クライアント
ユーザ
クライアント
アプリケーション
ブラウザ
ショップ
サーバ
コンテンツ
サーバ
ライセンス
サーバ
管理
システム
(B)購入、
再生処理
(21)コンテンツダウンロード要求(CID)
(22)コンテンツダウンロード(コンテンツ)
(23)利用権情報(Usage Right)要求(UID, Leaf−ID, TID)
(24)注文照会
要求(UID, TID)
(25)注文照会
応答(UID, 利用
条件)
(26)利用権情報(Usage Right)発行(Usage Right)
(27)再生要求
(CID, UID)
(28)再生処理

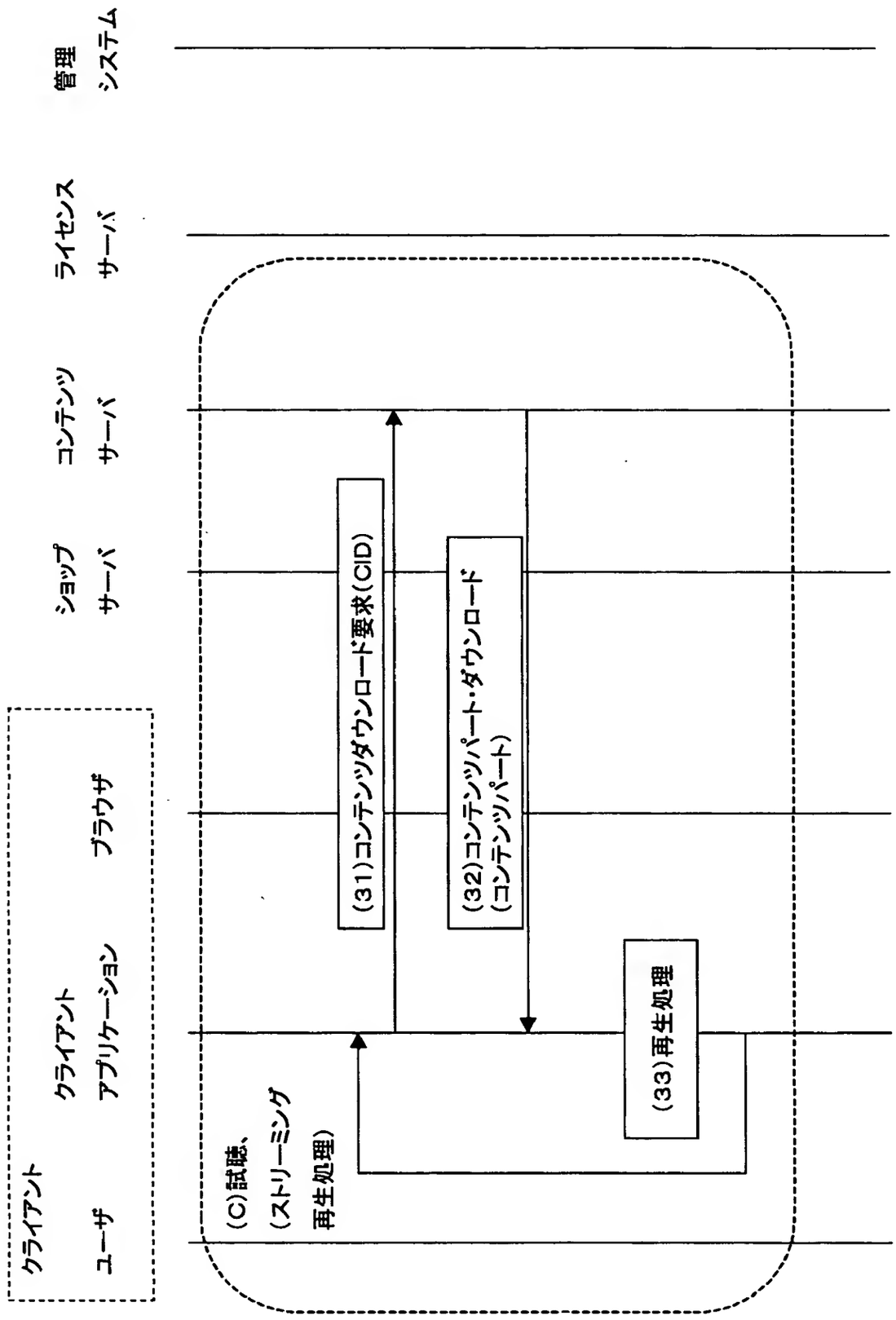
【図１９】


384
Enc(Kc, Content)
Content
382
コンテンツサーバ
Enc(Kroot, Kc)
Kc
EKB
Kroot
コンテンツファイル
試聴フラグ
サービスID
DNK
381
ライセンスサーバ
クライアント
383

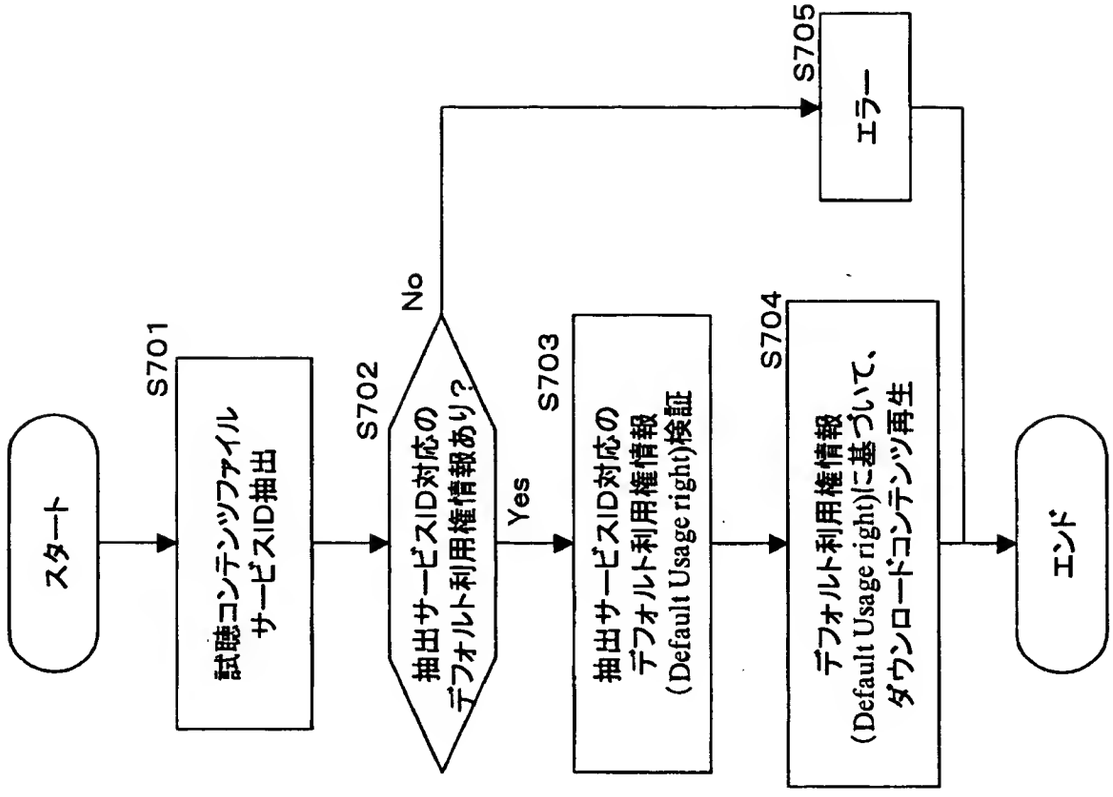
【図２０】


411
EKB(H)
(格納キー:Kroot')
412
HDNK
S501
EKB(H)
復号処理
Kroot'
S502
E(Kroot', SDNK)
復号処理
SDNK
S503
EKB(S)
復号処理
Kroot
S504
E(Kroot, CID+Kc)
復号処理
Kc
S505
マッチング
処理
CID
S506
E(Kc, Content)
復号処理
コンテンツ
(Cont nt)
401
サービスデータ
リーフID
EKBバージョン
E(Kroot', SDNK)
402
コンテンツファイル
サービスID
試聴フラグ
EKB(S)
(格納キー:Kroot)
E(Kroot, CID+Kc)
E(Kc, Content)
403
購入コンテンツ対応
利用権情報
リーフID
利用条件情報
CID

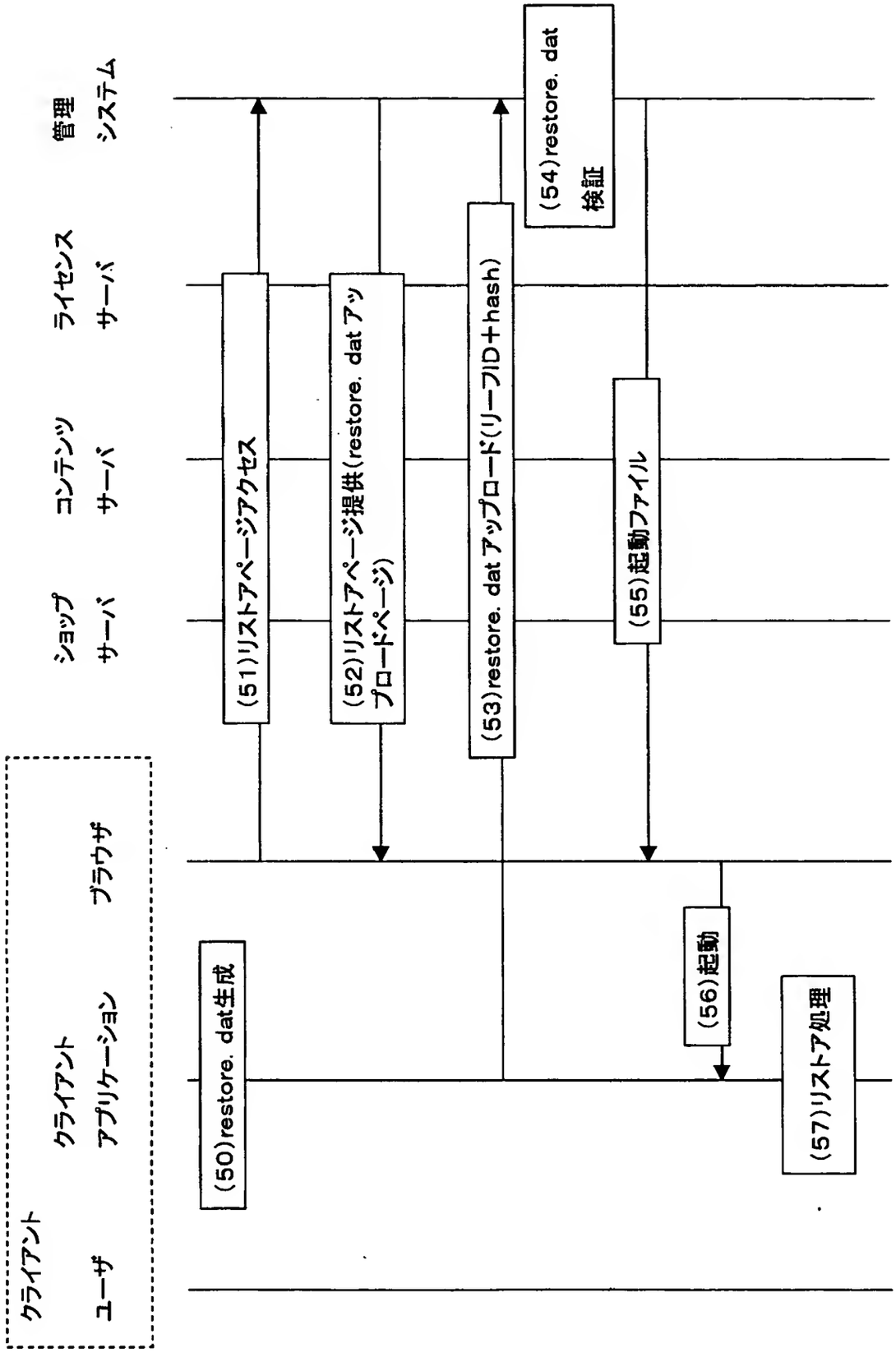
【図２１】


クライアント
ユーザ
クライアント
アプリケーション
ブラウザ
ショップ
サーバ
コンテンツ
サーバ
ライセンス
サーバ
管理
システム
(C)試聴、
(ストリーミング
再生処理)
(31)コンテンツダウンロード要求(CID)
(32)コンテンツパート・ダウンロード
(コンテンツパート)
(33)再生処理

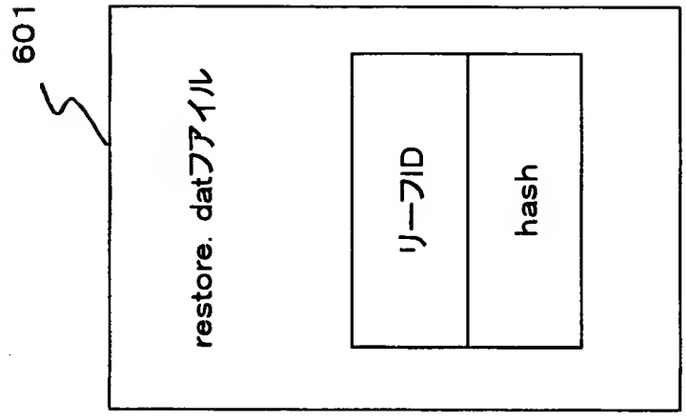
【図２２】


スタート
S701
試聴コンテンツファイル
サービスID抽出
S702
抽出サービスID対応の
デフォルト利用権情報あり?
No
Yes
S703
抽出サービスID対応の
デフォルト利用権情報
(Default Usage right)検証
S704
デフォルト利用権情報
(Default Usage right)に基づいて、
ダウンロードコンテンツ再生
S705
エラー
エンド

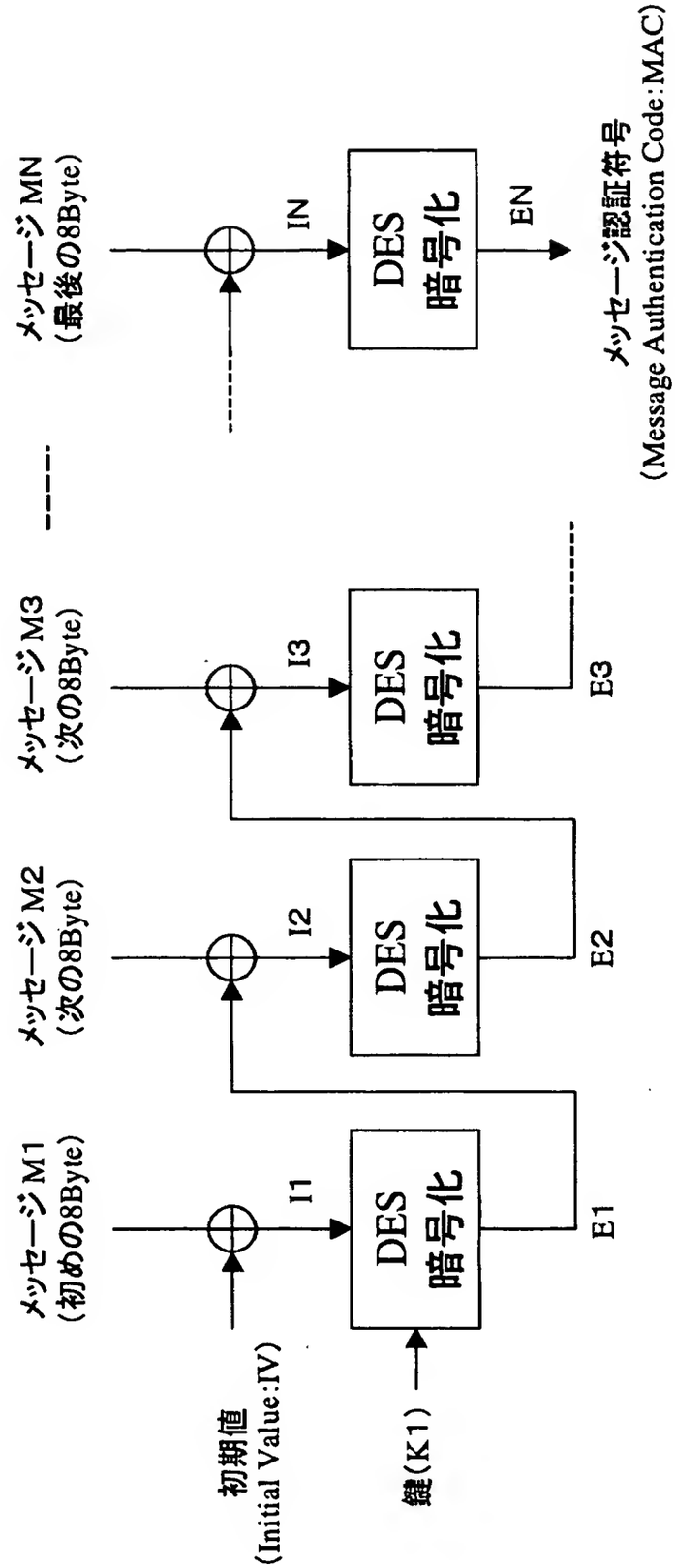
【図２３】


クライアント
ユーザ
クライアント
アプリケーション
ブラウザ
ショップ
サーバ
コンテンツ
サーバ
ライセンス
サーバ
管理
システム
(50)restore. dat生成
(51)リストアページアクセス
(52)リストアページ提供(restore. dat アップロードページ)
(53)restore. dat アップロード(リーフID+hash)
(54)restore. dat 検証
(55)起動ファイル
(56)起動
(57)リストア処理

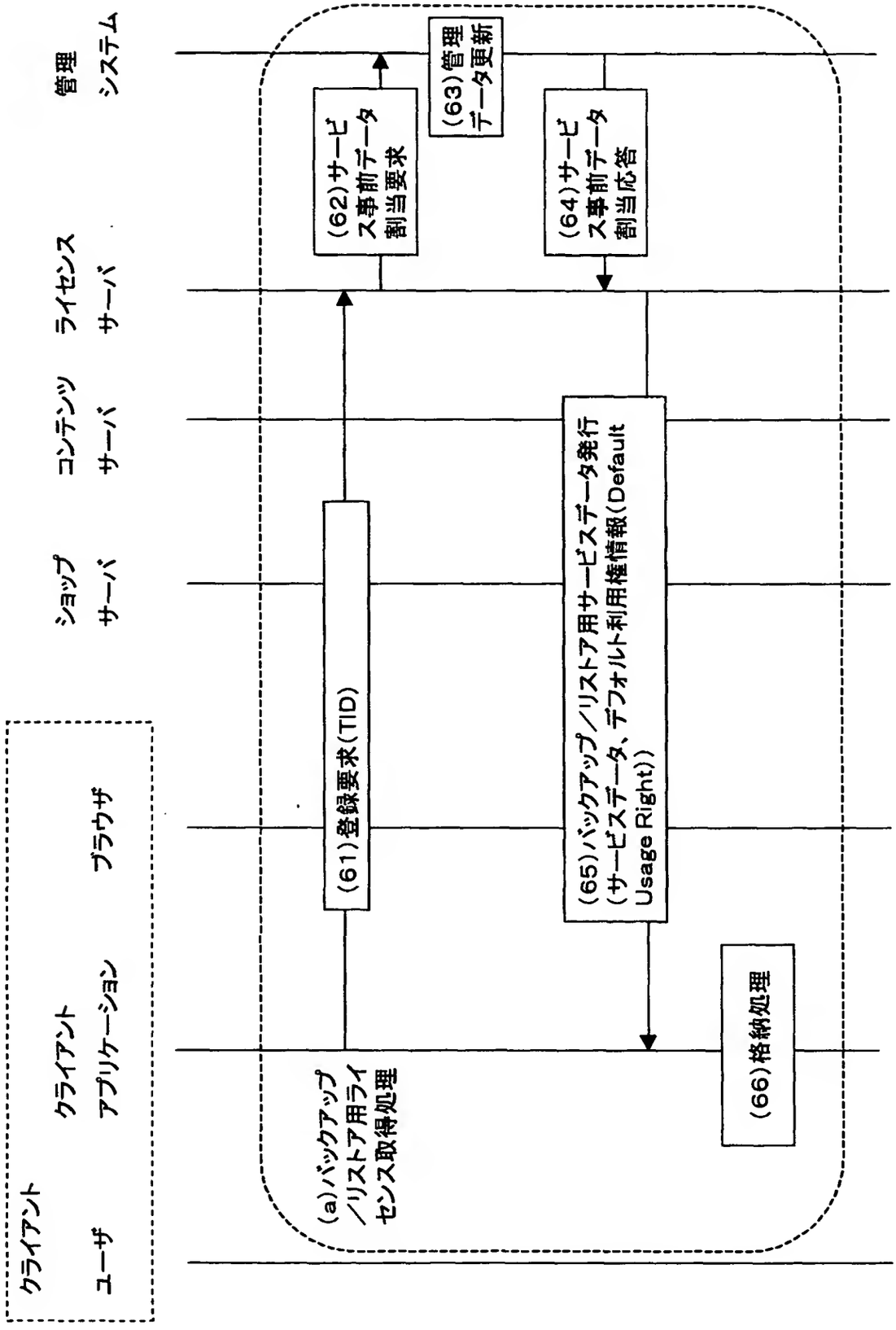
【図２４】



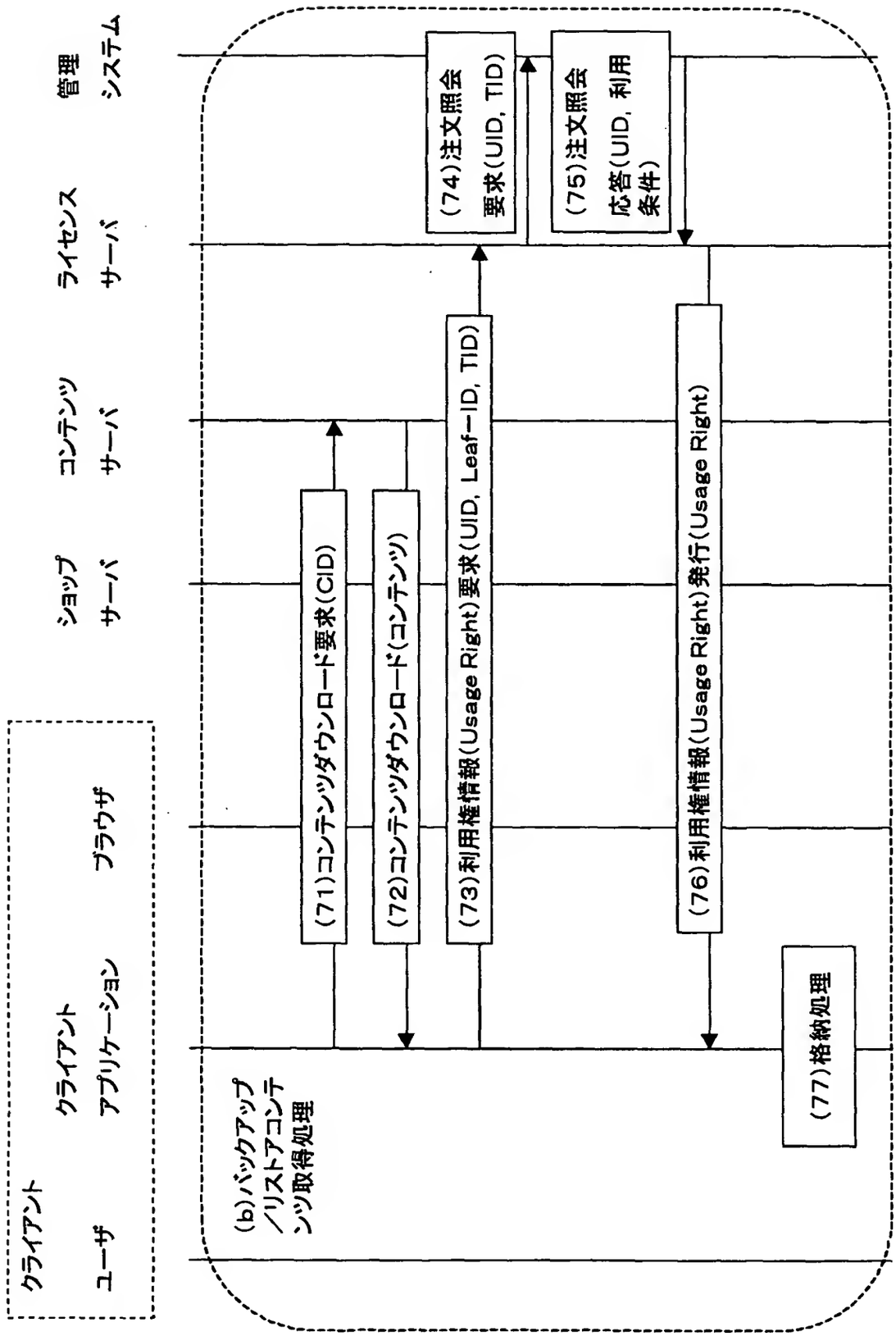
【図２５】


メッセージ M1
(初めの8Byte)
メッセージ M2
(次の8Byte)
メッセージ M3
(次の8Byte)
メッセージ MN
(最後の8Byte)
初期値
(Initial Value:IV)
鍵(K1)
I1
I2
I3
IN
DES
暗号化
E1
E2
E3
EN
メッセージ認証符号
(Message Authentication Code:MAC)
:排他的論理和処理(8バイト単位)

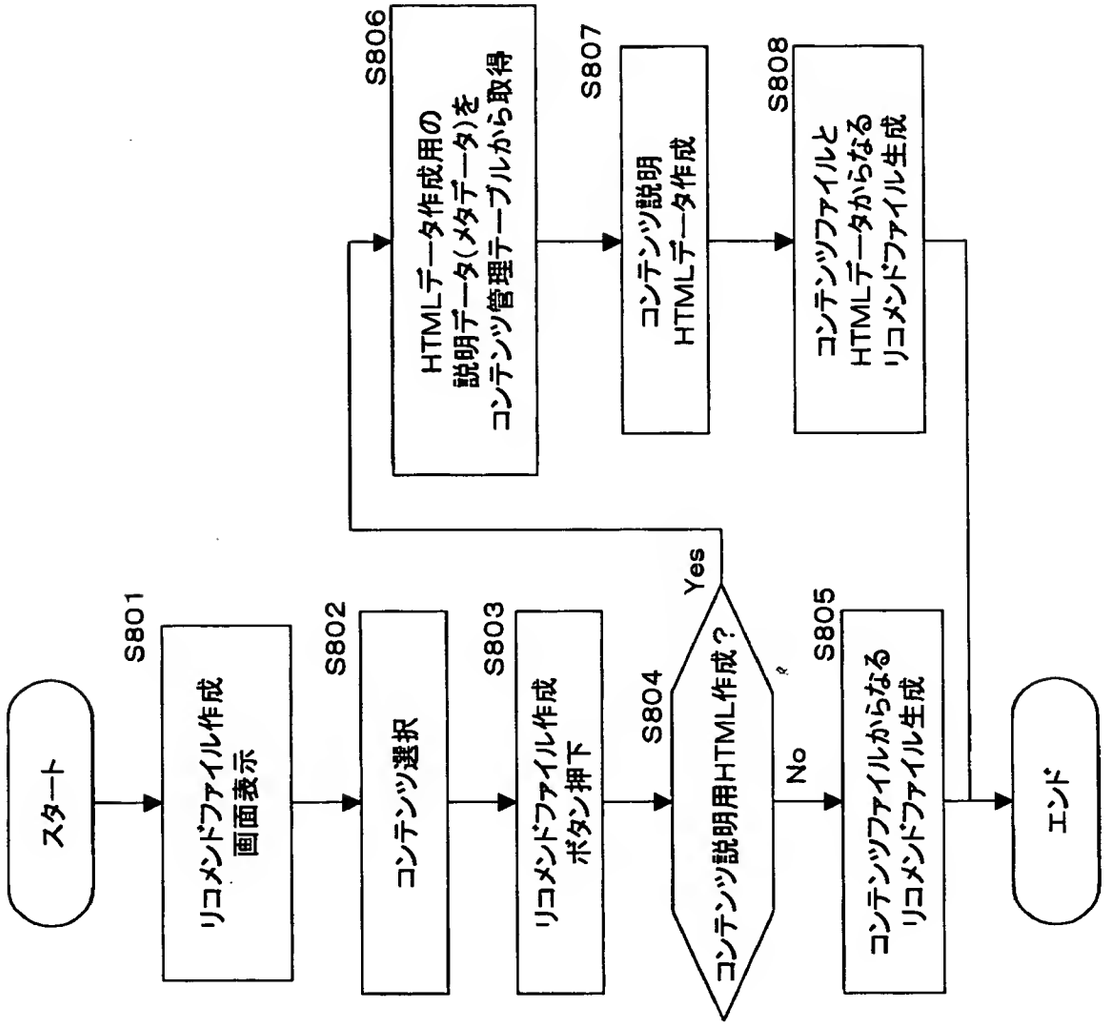
【図２６】


クライアント
ユーザ
クライアント
アプリケーション
ブラウザ
ショップ
サーバ
コンテンツ
サーバ
ライセンス
サーバ
管理
システム
(a)バックアップ／リストア用ライセンス取得処理
(61)登録要求(TID)
(62)サービス事前データ割当要求
(63)管理データ更新
(64)サービス事前データ割当応答
(65)バックアップ／リストア用サービスデータ発行(サービスデータ、デフォルト利用権情報(Default Usage Right))
(66)格納処理

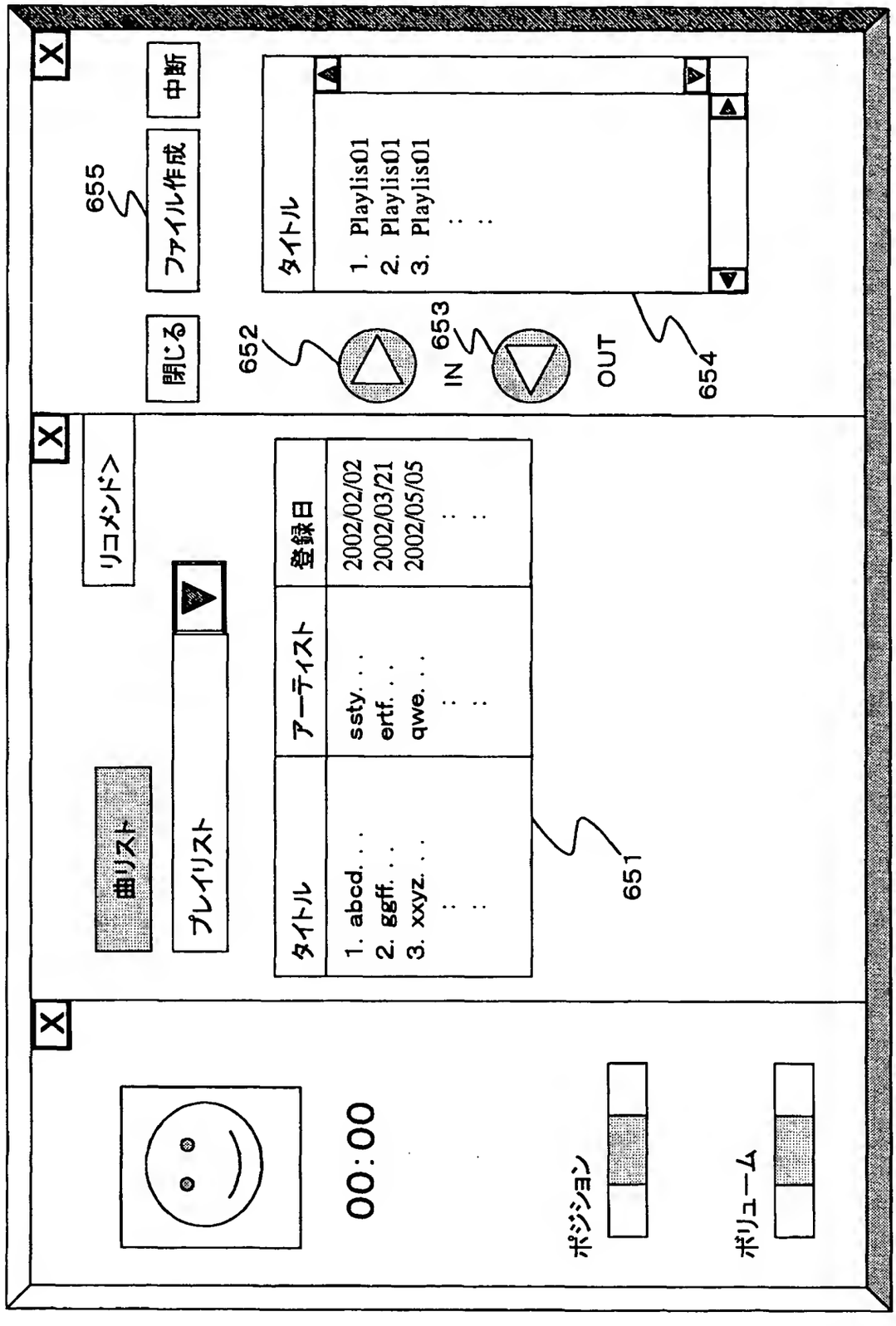
【図２７】


クライアント
ユーザ
クライアント
アプリケーション
ブラウザ
ショップ
サーバ
コンテンツ
サーバ
ライセンス
サーバ
管理
システム
(71)コンテンツダウンロード要求(CID)
(72)コンテンツダウンロード(コンテンツ)
(73)利用権情報(Usage Right)要求(UID, Leaf−ID, TID)
(74)注文照会
要求(UID, TID)
(75)注文照会
応答(UID, 利用
条件)
(76)利用権情報(Usage Right)発行(Usage Right)
(77)格納処理
(b)バックアップ
／リストアコンテ
ンツ取得処理

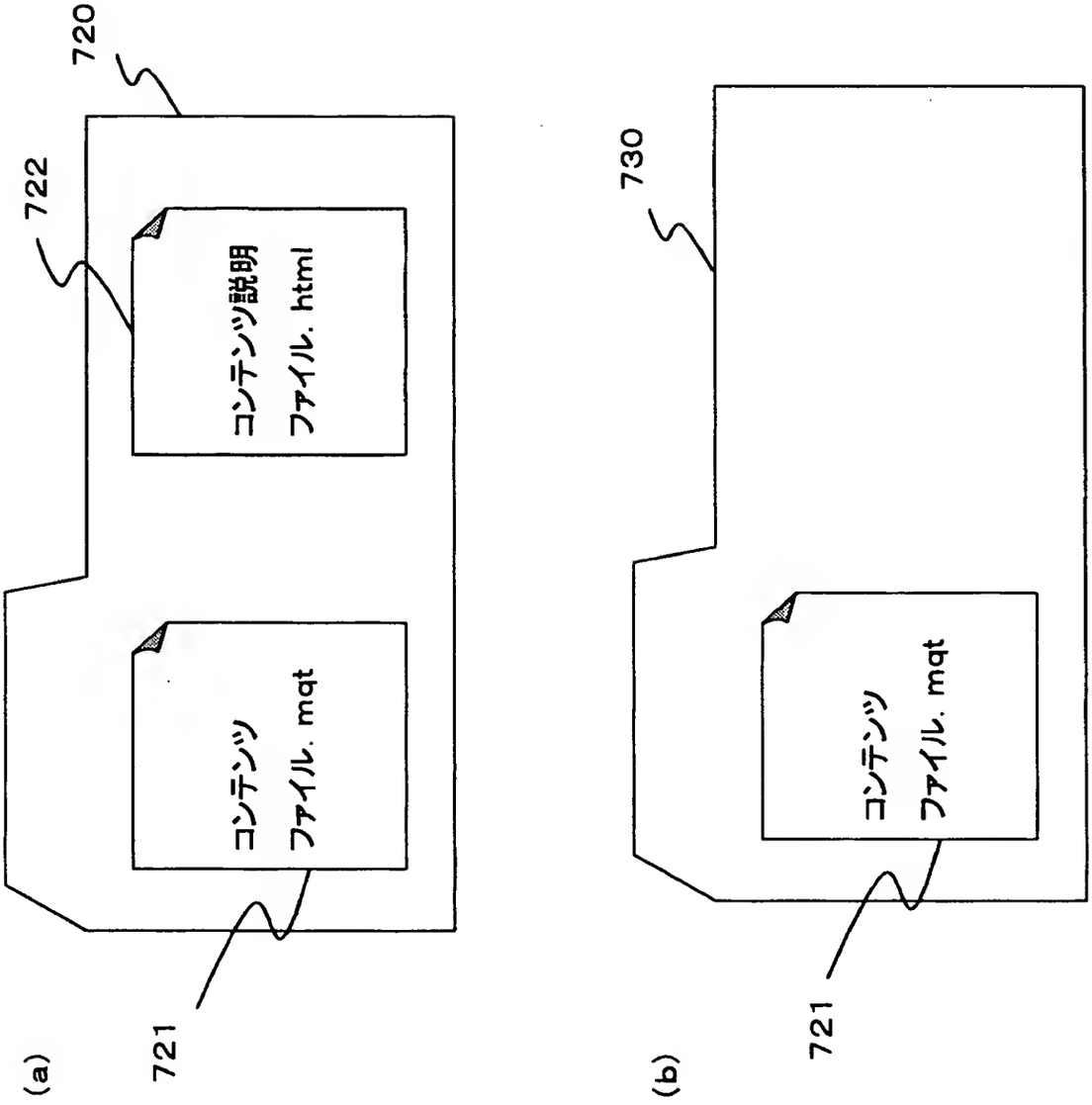
【図２８】


スタート
S801
リコメンドファイル作成
画面表示
S802
コンテンツ選択
S803
リコメンドファイル作成
ボタン押下
S804
コンテンツ説明用HTML作成？
Yes
No
S805
コンテンツファイルからなる
リコメンドファイル生成
エンド
S806
HTMLデータ作成用の
説明データ(メタデータ)を
コンテンツ管理テーブルから取得
S807
コンテンツ説明
HTMLデータ作成
S808
コンテンツファイルと
HTMLデータからなる
リコメンドファイル生成

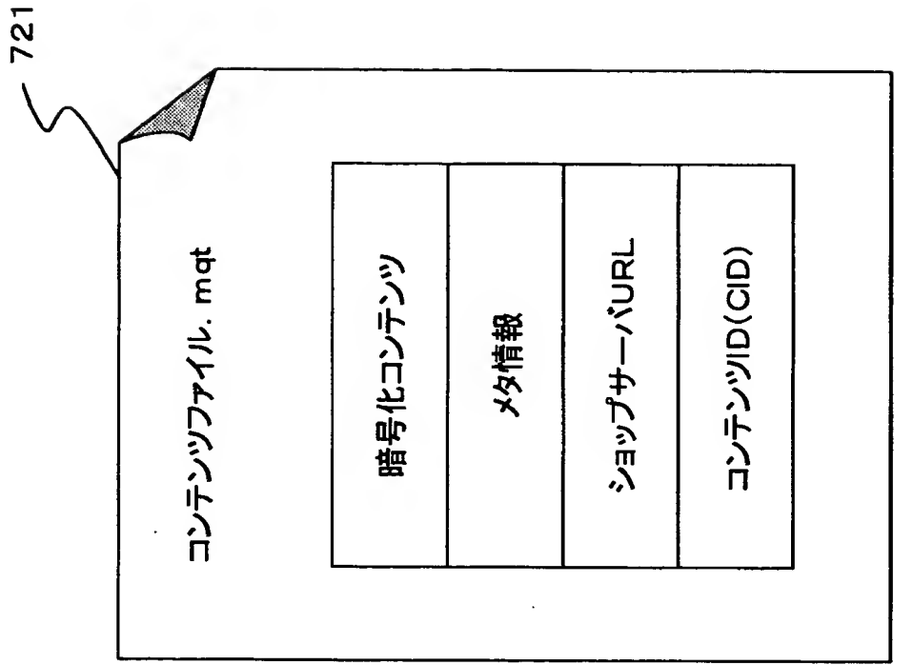
【図２９】


X
X
X
中断
ファイル作成
閉じる
655
652
653
654
IN
OUT
タイトル
1. Playlist01
2. Playlist01
3. Playlist01
リコメンド>
曲リスト
プレイリスト
タイトル
アーティスト
登録日
1. abcd. . .
2. ggff. . .
3. xxyz. . .
ssty. . .
ertf. . .
qwe. . .
2002/02/02
2002/03/21
2002/05/05
651
00:00
ポジション
ボリューム

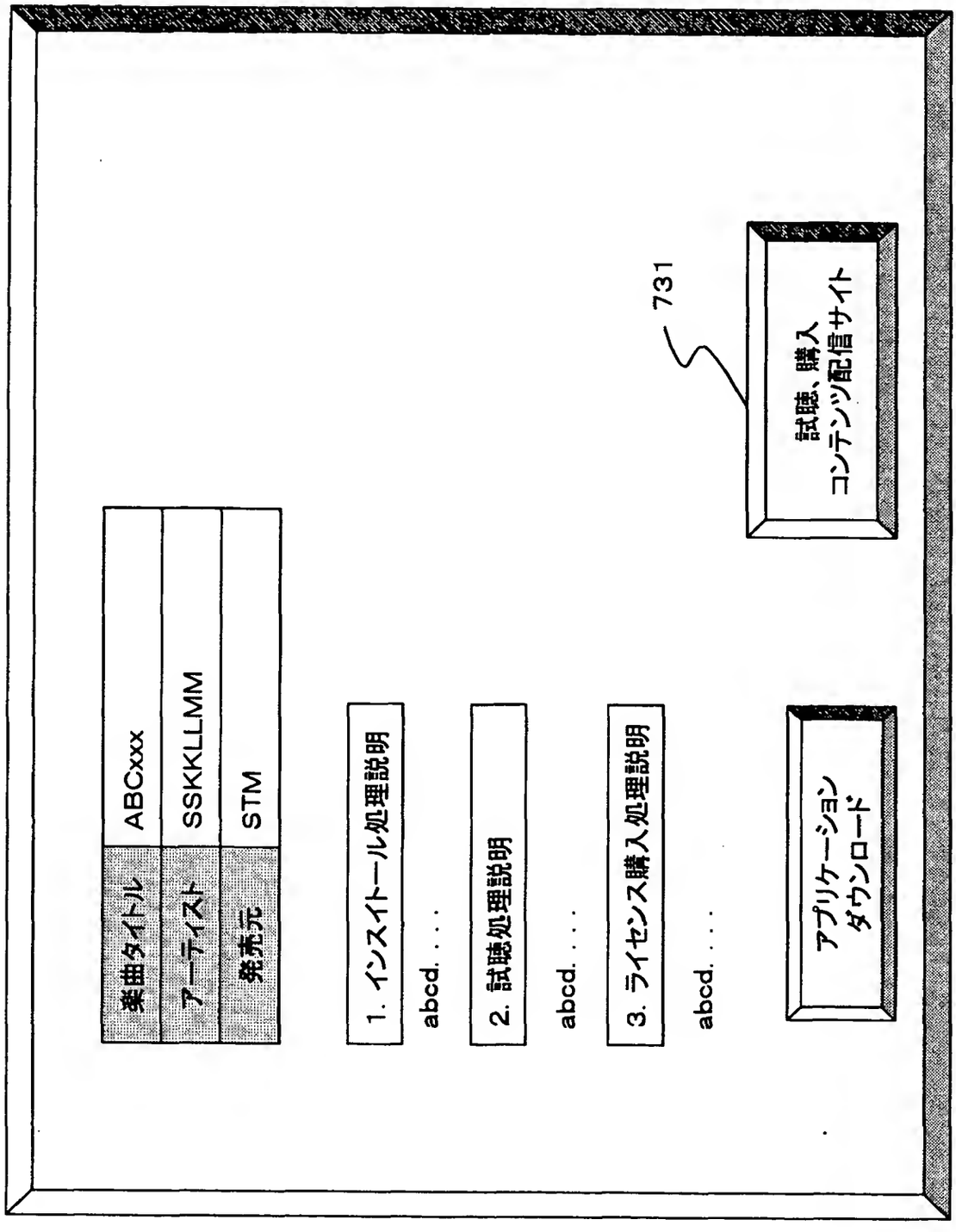
【図３０】


720
722
コンテンツ説明
ファイル. html
コンテンツ
ファイル. mqt
721
(a)
730
コンテンツ
ファイル. mqt
721
(b)

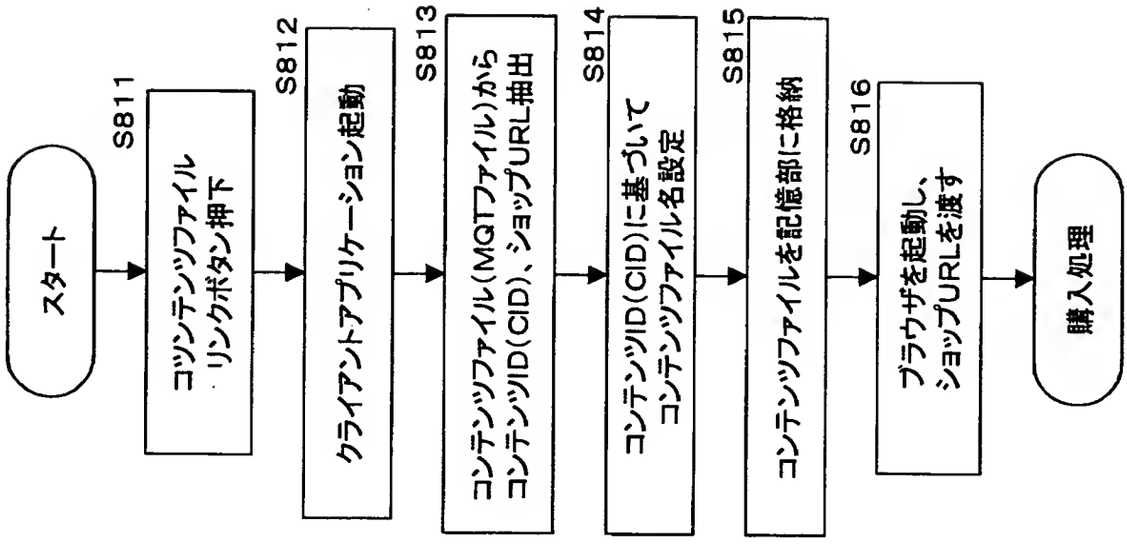
【図３１】



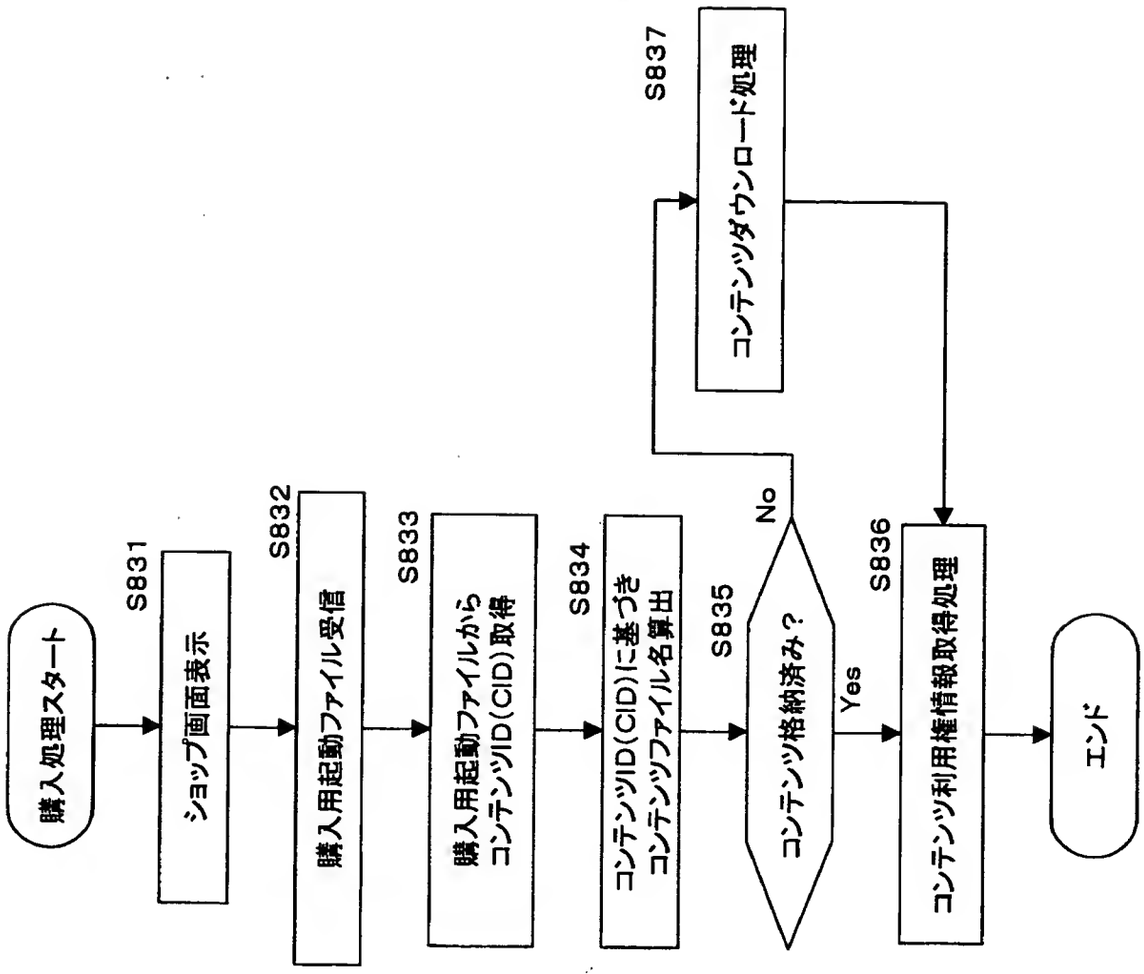
【図３２】


楽曲タイトル
ABCxxx
アーティスト
SSKKLLMM
発売元
STM
1. インスイトール処理説明
abcd. . . .
2. 試聴処理説明
abcd. . . .
3. ライセンス購入処理説明
abcd. . . .
アプリケーション
ダウンロード
731
試聴、購入
コンテンツ配信サイト

【図３３】


スタート
S811
コンテンツファイル
リンクボタン押下
S812
クライアントアプリケーション起動
S813
コンテンツファイル(MQTファイル)から
コンテンツID(CID)、ショップURL抽出
S814
コンテンツID(CID)に基づいて
コンテンツファイル名設定
S815
コンテンツファイルを記憶部に格納
S816
ブラウザを起動し、
ショップURLを渡す
購入処理

【図３４】


購入処理スタート
S831
ショップ画面表示
S832
購入用起動ファイル受信
S833
購入用起動ファイルから
コンテンツID(CID)取得
S834
コンテンツID(CID)に基づき
コンテンツファイル名算出
S835
コンテンツ格納済み？
No
Yes
S836
コンテンツ利用権情報取得処理
S837
コンテンツダウンロード処理
エンド

【書類名】　　要約書

【要約】

【課題】　コンテンツまたはライセンス情報のバックアップ／リストア処理をセキュアに実行する装置、方法を提供する。

【解決手段】　購入済みのコンテンツまたはライセンス情報としてのサービスデータ、または利用権情報を、正規なコンテンツ購入クライアントであることの確認を条件として、再取得可能とした。有効化キーブロック（ＥＫＢ）配信ツリーにおけるクライアント識別子としてのリーフＩＤおよび、該リーフＩＤに対する検証データを持つリストア処理要求ファイルをクライアント識別データとして適用する構成としたので、正規なコンテンツ購入クライアントであることの確認が確実に実行される。

【選択図】　図２３

出　願　人　履　歴　情　報

識別番号　　〔０００００２１８５〕

１．変更年月日　　１９９０年　８月３０日
［変更理由］　新規登録
住　所　　東京都品川区北品川６丁目７番３５号
氏　名　　ソニー株式会社